CYBERSPACE
IMPLICATIONS FOR U.S. DOMAIN WARFARE AND SINO RELATIONS

by
Eric Allen Slate

A thesis submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Arts in Global Security Studies

Baltimore, Maryland
December 2014

ABSTRACT

The predominate cyber discourse has focused on the impact of information theft as it relates to personal banking and financial data with occasional journalistic exploration of cyber enabled industrial and defense related intellectual property theft informing economic and national defense circles. To date, little work has been published which explores the economic and international relations implications of cyberspace, and the associated exploitation of it, as it relates to obtaining advantage, military or economic, in the production of high-technology and defense related goods. Even more simplistically little research has been done which examines cyberspace as a warfare domain for national security with a critical eye.

Cyberspace allows for the storage of vast amounts of data virtually, the global transmission of this same data quickly and efficiently, and theft of this data easily if ill protected. The complete economic impact of this lost intellectual property to technological superiority and national defense is not yet fully understood, although the simple monetary assessments of its loss are beginning to be discussed.

This thesis aims to add to this understanding by examining the evolution of cyber power exploring it as a domain for U.S. war, current impediments to the recruitment of U.S. cyber professionals also known in defense circles as cyber warriors, and the use of cyberspace by the People's Republic of China as a means of enabling intellectual property theft. These focus areas were researched as a means to develop the idea of cyberspace warfare. The inquisitive logic stream aimed to answer three questions:

(1) Is cyberspace an operational domain for U.S. warfare? (2) How does the U.S. recruit its warriors who fight and defend in cyberspace? (3) Who is an enemy or target of cyber war?

The body of this work concluded that cyberspace is not currently an operational domain of warfare, as it has been traditionally defined, but is a developing area that seems to be domain-like. The term domain-like was chosen to describe the current state of cyberspace as it relates to U.S. warfare due to the preponderance of cyber associated and attributed activity being leveraged as enabling functions to influence and shape actions and the environment prior conflict.

The influence fight in the context of cyber can be defined as the capability to leverage cyberspace as an enabler for traditional efforts within the physical domains of land, sea, air and space. For examples cyberspace is leveraged to obtain intellectual property, a feat that traditionally would have been done by acquiring a business sector through purchase or acquiring said intellectual property through espionage. Further research will be needed to examine the implications of growing cyber capability if its use becomes attributed to defensive or offensive military operations as an enabling or potentially integrated capability to operational domain warfare, and if the demonstrated capability becomes linked to a specific force or nation state.

Additional areas of research should examine the impact of technology growth and proliferation as fostered by the theft of large amounts of high-technology information via cyber exploitation. This work could help explore the implications of the proliferation high-technology information and industry trade secrets to current U.S. exports in high-technology and defense related areas.

It should be noted that the proliferation of the technical knowledge behind "the bomb" to the Soviets took years, and was undermined by several high-profile espionage cases (Gold, Greenglass, Fuchs, Rosenberg). It may now be possible to transfer this same type of technical knowledge, albeit separated throughout several industrial areas and defense base contractors, remotely via cyberspace with little to no public attribution or knowledge of its loss.

Thesis Advisors: Dr. Benjamin Ginsberg and Prof. Sarah Clark
Readers: Dr. Michael Warner and Dr. Kevin Woods

ACKNOWLEDGEMENTS

I wish to thank my family, friends, colleagues and professors at Johns Hopkins University for their support as I balanced working and attending the Global Security Studies program full-time. Without your understanding the research and work herein would not be possible. I would like to especially thank my husband Juan and best friend Damian for the countless hours you spent supporting me through this program and thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

How is cyberspace changing modern defense? This question has spurred many discussions, studies, and even the establishment of new military commands worldwide in the last decade. In examining this question, this thesis aims to deconstruct the major issues surrounding cyberspace as a means to better understand how they are affecting modern defense.

This topic is explored by examining three key questions, which correspond to chapters two, three, and four of this work in order. These questions are:

(1) How does the evolution of cyberspace compare with aerospace as it relates to U.S. military demonstrations of domain power (i.e. cyber power versus air power)?

(2) How does the U.S. Department of Defense compete with the private sector in the recruitment of the technical expertise needed to develop cyber warriors?

(3) How does the Peoples Republic of China's strategic Five-Year Plans drive their exploitation of cyberspace**?**

Firstly, this work examines cyberspace as a domain of warfare akin to land, sea, air, and space exploring whether it is or is not the latest addition. Exploring this concept proves exceptionally important to this study, as all current defense discourse asserts that cyberspace is in deed the fifth operational domain of warfare. However, contrary to this assertion this work concludes that cyberspace is not yet an operational domain of warfare in the traditional sense, but domain-like, the details of which are explored in the following chapter.

Secondly, as a means to better understand cyberspace as a United States Department of Defense warfare domain, chapter three explores the recruitment of U.S. cyber warriors. What better way to understand the defense aspects of cyberspace than to

examine the expertise and background of those individuals being recruited to fight its wars and defend its assets? Although, there was not a lot of information readily available within this topic area, the research was able to identify key impediments that may restrict or hinder the diverse recruitment of future warriors.

Thirdly, to examine a possible adversary within cyberspace and how that adversary is leveraging cyberspace to wage war, chapter four explores The People's Republic of China's (PRC) exploitation of cyberspace. The findings in deed show that the PRC is exploiting cyberspace, but uncovers no direct linkages to or evidence of cyber weapons, but instead intellectual property theft in the guise of state sponsored corporate espionage. Does this further support the findings that cyberspace is domain-like, and being used for the influence fight as an enabler?

In concert, the various finding of this study help to add to the discourse of national defense on this topic exploring concepts of traditional kinetic warfare and deterrence in comparison to national enabling functions for defense and overall state advantage.

Overall this thesis argues that for cyberspace to be a true operational domain of warfare, akin to land, sea, air, or space, in the traditional sense, that credible and attributed capability to an actor must be demonstrated in order for said capability to have a military coercive or deterrent effect that could be leveraged by policy makers. Further, as it relates to defense and deterrence, it is paramount for offensive or defensive military manipulation of cyberspace as a weapon or tool of war and statecraft to be surmised or known, and demonstrated or credible, in order for it to begin to earn a level understanding as a distinct military capability. Simply leveraging cyberspace to obtain

information or steal secrets, an evolution of espionage tradecraft and not warfare, does not constitute a new operational domain of warfare, as has been argued and stated in strategic global defense communication.

CHAPTER 2: A COMPARATIVE ANALYSIS OF THE DEVELOPMENT OF INTER-BELLUM AIR POWER AND CONTEMPORARY CYBER POWER

"Cyber security threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."

- 2010 National Security Strategy

Global Internet usage has increased by more than 550% in the last decade, with over two billion people worldwide accessing cyberspace [1] daily.[2] Since the Internet's adolescence in the mid-1980s, it and cyberspace have often been viewed as little more than a conglomerate of disparate networks and servers, or an abstract technological domain. [3] Often, little thought is given to how cyberspace is changing human interaction.

In today's world, the Internet and cyberspace encompass the sole artificial reality in which mankind interacts. In this reality, the digital language of ones and zeroes, yes and no, connects the creator to his creations often leveraging pre-existing

[1] The definition of cyberspace varies greatly with Webster's Dictionary defining the word as "the realm of electronic communication," and Collins Dictionary defining it as "all of the data stored in a large computer or network represented as a three-dimensional model through which a virtual-reality user can move." The U.S Department of Defense defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The definition of cyberspace pursued in this study includes parts of the above descriptions. For the purpose of this discussion cyberspace will be defined, as a three-dimensional virtual reality comprised of networked hardware and software used for human-to-human, human-to-machine, or machine-to-machine electronic communication and or control analogous to the Internet in most conversations.

[2] Department of Defense, United States of America, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, 1, Accessed April 11, 2013, http://www.defense.gov/news/d20110714cyber.pdf.

[3] Jason Healey, editor, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 2013., 8.

communications architecture such as telephone lines as an ever-growing network of fiber optic and wireless technology is created. This is communication at the speed of light.

In spite of its' synthetic origins and predominantly intangible nature, cyberspace has been labeled as a new operational domain for warfare within military and government discourse. [4] The label of domain has predominantly been saved for tangible reality in which man can physically maneuver or manifest. Regardless of its uniqueness and virtual characteristics, cyberspace now fosters immense human interaction, while simultaneously embodying and reinforcing complex social networks, linking people from varied backgrounds and locations globally.

Cyberspace is and will continue to be a fundamental part of globalized Twenty-first Century life. Understanding the implications of cyberspace in the context of national security, [5] international relations, and warfare will become increasingly important in the coming decades as the Global War on Terrorism and current U.S. forward presence and power projection becomes increasingly difficult to sustain. Cyberspace offers opportunities for cost reductions if it can be operationally applied as a tool to foster a militarized virtual forward presence in support of U.S. interests.

If the United States can successfully integrate and demonstrate the militarization of cyberspace into existing operational domains of warfare such as land, sea, air, and space, it may find a means to reduce military costs. These cost reductions could be

---

[4] *Department of Defense Strategy for Operating in Cyberspace*, Washington, DC: U.S. Department of Defense, 2011., 5.

[5] For this research focus will be given to the implications of cyberspace as it relates to the national security of the United States, leveraging examplars from other areas for comparison, although these findings will be able to be applied to most other nations whose militaries are based on the joint construct of the United States' services (Army, Navy, Marines, Air Force etc.).

associated with a decrease in basing troops overseas and acquiring traditional kinetic weapons. Forward basing of troops and traditional weaponry has historically been focused on limiting an adversary's means to logistical support and sustain war.

The operational use of cyberspace as a domain to support war offers a revolution in military affairs. Instead of focusing on bombing industry and destroying lines of communication and logistics, tactics developed during the Napoleonic and World Wars, states can now make technology and communication inoperable by employing and exploiting weaknesses in the networks that connect weaponry, technology, and society.

This study will investigate whether cyberspace is in fact a new operational domain for national security. It is important to determine if cyberspace is an operational domain akin to the traditional domains of land, sea, air, and space, in order to assess the capability of the United States to integrate the emerging and evolving doctrine surrounding technology and cyberspace into traditional warfare. This research will also attempt to identify parallels in the development of warfare policy as a means to potentially project future national security implications involving cyberspace.

Specifically, the body of this work will focus on comparing and contrasting similarities between the developments of the domain doctrines of air and cyberspace as a means to support or refute the U.S. characterization of cyberspace as an operational domain. [6] In so doing it is hoped that this work will highlight that cyberspace does not need to be classified as an operational domain in order to support national security. In

[6] Operational domain doctrine is the literature surrounding the use of a domain to achieve an objective often in support of national security. Within government and military writings once this doctrine has been proven and demonstrated it is often known as domain power i.e. air power, cyber power etc.

fact, the stove piping of various capabilities into distinct operational domains can serve more as a hindrance then an enabler in the creation of unified joint doctrine for war.

Literature Review

"Aeronautics opened up to men a new field of action, the field of the air. In so doing it of necessity created a new battlefield; for wherever two men meet, conflict is inevitable."

- Giulio Douhet, *The Command of the Air,* 1921

The world has quickly integrated the power of the Internet and cyberspace, to include associated hardware, software, computing and networking, into daily life. Cyberspace and the Internet are ubiquitous to the majority of the public. Cyberspace traditionally connotes technical architecture and systems engineering, while the Internet tends to be the laypersons entre into cyberspace. Cyberspace and the Internet both promote the sharing of ideas, the proliferation of technology, and the growth of commerce worldwide.

In the United States, cyberspace connects "energy, banking and finance, transportation, communication, and … Defense Industrial Base" sectors with the global economy. [7] The immediate connectivity cyberspace has brought to the world encompasses the breadth of global commerce and logistics.[8] The high-speed communication and networks created by the Internet has spurred globalization, linking geographically separated and disparate physical realities (public and private tools, buildings, remote locations to public and private networks) to one another. The

[7] *Department of Defense Strategy for Operating in Cyberspace*, Washington, DC: U.S. Department of Defense, 2011., 1-2.

[8] Commerce in this context includes the human and compute- to-computer communication, logistics, and transactions involved in banking, production, trade, and defense.

connectedness brought by networking logistical hubs with command and control has been embraced by all sectors and has spurred new areas of communication and cooperation. This, coupled with cyberspace's centrality to contemporary life has spurred national security sectors of world governments to explore cyberspace as a new operational domain to "organize, train, and equip" defense capabilities. [9]

The United States and other nations are organizing and creating government and military command structures focused on "synchronizing and coordinating" efforts in cyberspace. [10] With nations and militaries defining cyberspace as a fifth operational domain, there are opportunities to study the development of cyberspace in parallel to the established fronts of land, sea, air, and space as a means to project the potential evolution of the use of cyberspace in support of traditional warfare. [11] In order to examine the reality of cyberspace as an operational domain in the context of U.S. national security, it is key to understand the breadth and scope of the accepted definition of an operational domain.

Within government and military literature operational domains are divided into areas focused on man's capability to maneuver in physical reality. Quite simply man can live on earth, transit the seas, fly through the air, and visit space. Traditional operational domain doctrine has focused on exploring the application of power to fulfill or aid national security historically within the material domains of land and sea and within the last century air and space. These domains have been further refined into the domains

[9] *Department of Defense Strategy for Operating in Cyberspace*, Washington, DC: U.S. Department of Defense, 2011, 5.

[10] Ibid., 5.

[11] Ibid., 5.

which constitute the global commons, sea, air, and space. Global commons are the domains considered vital to international trade and commerce, of which national sovereignty only governs limited areas. [12]

The works of air power theorists, such as Italian, Giulio Douhet (1869-1930), and American, William Mitchell (1878-1936), provide great examples of doctrine developing organically based on man's growing and evolving capability to maneuver within physical reality. As new air capabilities developed (balloons, powered air craft, fighter aircraft, bombers etc.) doctrine evolved to address new capabilities or exploit newly discovered weaknesses. This doctrinal development approach also works where doctrine out paces current technology, spurring technologic development to meet hypothetical doctrine. As an example theorists propose strategic bombardment before the advent of bombers, and long-range bombers are created to answer the theory. This example actually occurred with Douhet and his proposition of strategic bombardment in the 1920s which technology at the time did not support. It was not until the 1940s that the long-range bombers of Douhet's vision became reality.

The development of doctrine, that is the literature that supports how to use a domain to wage war, helps to operationalize domains in support of national security objectives. This can be seen in the development of air doctrine and its integral nature in the operational use of airspace in warfare. By advocating for the strategic bombardment of nations by air, as a means to break civilian morale and thus diminish a nation's capability to wage war, theorists such as Douhet, opened up the possibility of airspace to

[12] For more insights and thoughts on the politics surrounding global commons you can refer to Peter Dauvergne's *Handbook of Global Environmental Politics.* Recent discourse has also begun to explore the Internet and cyberspace as a new global commons.

be used as a new to support national security. [13] In creating warfare doctrine for new technologic advancements (i.e. manned flight) theorists are able to repurpose what may have been viewed as science fiction into a real world operational context. The use of aircraft during the World Wars was the anointment of the emerging domain of airspace as an operational domain, in support of national security thus creating new opportunities for to evolve and support traditional warfare.

The creation of an operational domain has traditionally meant that capabilities of that domain have been proven. Proven capabilities, based in the theory and doctrine of the domain are normally tested during war, and subsequently bring domain theory into fruition, shifting doctrine to a measurable form of power which can be demonstrated.

Despite nations the world over declaring cyberspace as a fifth operational domain there remains dissenting views that cyberspace, in part due to its man-made nature and unproven operational doctrine, is not a new domain, but merely a new way of connecting and communicating between the traditional domains. This is true; none of the other domains can strategically connect and affect all domains like cyber can. Although artificial by nature, cyberspace is able to connect and affect all man-made capabilities that are networked, both by wire and wirelessly, within all other operational domains. This capability makes cyberspace and cyber power unique in comparison with the traditional domains of land, sea, air, and space.

The U.S Department of Defense (DoD) explicitly defines air and maritime domains, focusing on their physical manifestations (i.e. the atmosphere, rivers and seas

[13] Giulio Douhet, *The Command of the Air*, Translated by Dino Ferrari, Washington, D.C.: Air Force History and Museums Program, 1998 (New York: Coward-McCann, 1942).

etc.) [14] These definitions, which are found in the Department of Defense Dictionary of Military and Associated Terms, predominantly focus on the physicality of the air and maritime domains.

As outlined in *On Cyberwarfare,* a Geneva Center for the Democratic Control of Armed Forces publication, the man-made nature of cyberspace and the cyber domain, make it exceptional in comparison to traditional definitions. [15] Besides connecting all other domains, cyberspace also cannot exist without its man-made architecture and components making its reality non-physical. If man were no longer to exist land, sea, air, and space would still be here. Conversely, unlike the other domains, cyberspace can be replicated innumerable times by replicating the infrastructure that supports it; the physical reality of man is (the earth of the land, the seas of the world etc.) is bound by the physical limitations of matter (man cannot create matter, only reorganize it). [16]

There are plentiful examples of national power expression within the traditional domains. These expressions of state power are often seen as the culmination of operationalizing a domain in support of national security; power being defined as the overt proven military demonstration of a capability in support of national interests or policy. Power is often solely proven in times of war, as power often tends to focus on destruction, and periodically re-demonstrated during times of peace, under the guise of military training exercises. This power re-demonstration additionally serves as a means

---

[14] *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms,* Washington D.C.: U.S. Department of Defense, as amended through 15 October 2013.

[15] Fred Schreier, *On Cyberwarfare,* Geneva Center for the Democratic Control of Armed Forces Horizon 2015 Working Paper Series, no. 7 (2012), 12.

[16] Ibid., 12.

of deterrence [17], reminding potential adversaries of the physical manifestations of capabilities whose effects may be so destructive that they are only showcased once or twice against human targets, as in the case of the atomic bomb.

Although the world knows cyberspace exists, and there has been reporting on "cyber attacks," as highlighted by the destruction of Iranian centrifuges at the Natanz nuclear facility, there has not been a proven attributable cyber power capability demonstrated. [18] The lack of attribution connected to a capability makes a demonstration of power impossible. Without proven and attributable power capabilities within cyberspace, one could argue that cyberspace is not an operational domain analogous to the traditional war hardened domains of land, sea, air, and space.

Although U.S. government policy is labeling cyberspace as the fifth operational domain of warfare, it may be more fitting to view cyberspace as an intangible addition to the global commons, supporting and facilitating communication within the traditional domains. [19] By translating physical reality into a global digital language, cyberspace connects the disparate and geographically separated technology of the world in ways telephone and its forbearer the telegraph could not.

Although there is ample literature on the development of aerospace as an operational domain, which examines aspects such as reconnaissance, strategic bombing,

---

[17] In order for deterrence to truly work the capability must be demonstrated and most importantly attributable, meaning adversaries must know you have the capability as well as a demonstrated willingness to use it.

[18] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York: Random House, 2012.

[19] Ibid., 13.

and nuclear deterrence post World War II, there remains little literature that is similar discussing cyberspace.

Although current literature and doctrine states cyberspace is a new operational domain akin to air we see little in traditional demonstrations of cyber power as we have with air power. This lack of state attribution and power demonstration, which undermines the argument that cyberspace is an operational domain, is not wholly negative to supporting the integration of cyberspace into the national security apparatus and consciousness. There have been ample examples of cyber power being demonstrated since the 1980s, although these examples have predominately been attributed to hackers. [20] The term hacker has become pejorative in the public domain often carrying a connotation of simple computer nerds "playing" in cyberspace.

Word choice in how we choose to describe cyberspace and the actors operating in it highlights the nuances that separate cyber crime from cyber conflict, attack, and war. These nuances have caused the current discourse surrounding cyberspace to become mired in the no man's land separating policing actions and national security often blurring the threat cyber conflict poses to national security if it is not fully integrated into joint military operations and capabilities.

This work will focus on identifying whether cyberspace is or is not an operational domain like aerospace. For cyber power to become a tool for national security states must openly demonstrate its power and destructive capability.

[20] Healey., 18.

Methodology & Hypothesis

"The very technologies that empower us to lead and create also empower those who would disrupt and destroy."

- 2010 National Security Strategy

After a thorough examination of the existing literature, exploring the arguments for and against cyberspace as an operational domain of warfare in pursing national security objectives, one major question stands out requiring further investigation. This question – How does cyberspace operationally compare against the defined warfare domains of land, sea, air, and space? – resulted in a study comparing and contrasting the development of air power with cyber power.

The air domain, including subsequent doctrine and power examples, was chosen as a benchmark for investigating cyberspace as an operational domain, due to it being the most recently proved operational domain of warfare. The air domain was also chosen for comparison because it is the only domain to which man had no previous access and subsequent access only through technology.

By conducting a comparative analysis of airspace with cyberspace, exploring the early development of air doctrine and its subsequent operational deployment in contrast to current cyber doctrine, I hope to use similarities and divergences to either support of refute the assertion that cyberspace is the fifth operational domain of warfare.

In this analysis I hope to find parallels in the early development and employment of manned flight in comparison with the use of cyberspace. This development should progress along similar paths since both airspace and cyberspace access is dependent on technology that must first be developed and explored, with subsequent doctrine being written in order to operationalize a suggested capability in support of warfare.

If there are sufficient parallels in the development and employment of airspace and cyberspace as domains, I should be able to map growth of capability in support of national policy and ultimately power projection. If the development of airspace maps with cyberspace, it should be possible to predict the future path for the application of cyber power while simultaneously supporting or refuting cyber as fifth operational domain of warfare. The development of capability may prove to be dependent or independent of creation of distinct domains, and should be recognized by the mapping of capabilities and counter capabilities to one another.

Data & Results

"History does not so much repeat as echo…"

- Lois McMaster Bujold, *A Fierce Domain*

The early evolution of cyberspace as compared to the domain of aerospace is very similar, particularly in examining the application of air power during the early 20th Century and *interbellum* periods. The use of aircraft prior to World War I (WWI) was extremely limited and viewed mainly as hobby and past time; there was little thought of the aircraft's military application when the Wright Brothers took flight in 1903. This is similar to the early development and application of the Internet by broad segments of the general public in the mid 1980s through 1990s (although the Internet's genesis can be found in the U.S. defense sector). The pilots of the early 20th Century, pre WWI, and the Internet surfers of the mid-1990s had similar goals, focusing on personal past time in the pursuit of pleasure for their hobby.

The progression of air power and cyber power has generally mirrored one another following a somewhat predictable course. This course, highlighted in the below graphic,

begins with a new technology or capability being developed. This capability is first used for reconnaissance, which then leads to its use as an offensive or attack capability (in part to deny or degrade reconnaissance), resulting in the development of defensive measures to deny attack from adversaries, which ultimately leads to the institutionalization of the myriad of capabilities in support of national security interests. The air power theory of WWI provides key context and details for this comparison.

	Reconnaissance	Attack	Defense	Organizational Adoption
Air Power	Aircraft used to spot targets	Development of attack aircraft and strategic bombers	Development of intercept aircraft to guard against attack and bombardment	U.S. Air Force
Cyber Power	Cyber intrusion used for espionage to support attack	Development of cyber tools to exploit technical weaknesses identified by cyber intrusion	Hardening of networks and software to deter and protect against intrusion and exploitation	U.S. Cyber Command

Table 1. Mapping of Air Power to Cyber Power

Following the outset of WWI the aircraft began to be looked at for its applications to war. Initially

> The great mobility and range of powered aircraft… led to their use in reconnaissance… Soon artillery spotter planes became a serious threat to troops on the ground. Since artillery specifically designed for use against aircraft had not been developed before the war, the only way to drive off interlopers intent on reconnoitering one's positions was to attempt to shoot them down with weapons – at first handguns and rifles, later machine guns – mounted on one's own aircraft. Thus the reconnaissance and pursuit roles [of aircraft] were the first [functions] to emerge clearly. [21]

With successful demonstrations of air power during war, leaders and air theorists began to discuss and debate the role and future growth of air power. The main discourse

[21] David MacIsaac, "Voices from the Central Blue: The Air Power Theorists." In *Makers of Modern Strategy: From Machiavelli to the Nuclear Age,* edited by Peter Paret. (Princeton, NJ: Princeton University Press, 1986, 628).

of the 1920s and 1930s built on the operational tactics developed during WWI. Theorists such as Italian, Giulio Douhet (1869-1930) and American, William Mitchell (1878-1936) debated the various aspects of air power. Douhet and Mitchell, who entered military service in their respective armies before the creation of flight, were the early lead proponents of air power and the aircraft's application as an instrument of war in support of national policy. [22]

Douhet's theory of air doctrine can be abbreviated as follows:

(1) modern warfare allows for no distinction between combatants and noncombatants

(2) successful offensives by surface forces are no longer possible

(3) the advantages of speed and elevation in the three-dimensional arena of aerial warfare have made it impossible to take defensive measures against an offensive aerial strategy

(4) therefore, a nation must be prepared at the outset to launch massive bombing attacks against the hard to shatter enemy civilian moral, leaving the enemy government no option but to sue for peace

(5) to do this an independent air force armed with long-range bombardment aircraft, maintained in a constant state of readiness, is the primary requirement. [23]

The wrestling of balance between defensive and offensive military capabilities, as outlined in Douhet's abbreviated theory of air doctrine, has striking similarities with the

[22] Edward Warner, "Douhet, Mitchell, Seversky: Theors of Air Warfare," In *Makers of Modern Strategy: Military Thought from Machiavelli to Hitler,* edited by Edward Earle. Princeton, NJ: Princeton University Press, 1948, 485.

[23] Op. Cit., David MacIsaac ,630.

current military dialogue of cyber doctrine development, and proposed operational application.

Current cyber doctrinal discussions recognize that defense of logistical command and control and infrastructure is an integral part of cyber policy and doctrine. [24] A defensive posture supporting vulnerable targets is one concept that echoes Douhet's fears that successful offensive capabilities of ground forces are no longer capable of outpacing a quick and highly mobile threat, as was the case with aircraft outpacing draft animal drawn and mechanized machinery during WWI. A similar track can be seen in the development of U.S. cyber defense organization in the mid 1990's and their militarization to focus on defensive as well as offensive operations in the early 2000s. [25]

Where Douhet proposed to counter diminishing defensive capabilities of traditional ground forces with heavy offensive strategic bombardment capability, the U.S. government is similarly adopting a declaratory deterrence policy as a means to support defense of the nation against cyber attack. [26]

The U.S. government is softening the strike first language of Douhet's air doctrine, which advocated strategic bombardment aimed at breaking civilian morale, by advocating a two pronged approach to deterrence. [27] First, the United States proposes to deny an adversary's use of cyber attack capabilities against it by hardening defensive

[24] Op. Cit., *Department of Defense Strategy for Operating in Cyberspace,* 6.

[25] Healey., 18.

[26] *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to National Defense Authorization Act for Fiscal Year 2011, Section 934*, Washington, DC: U.S. Department of Defense, 2011, 2.

[27] Ibid., 2.,

capabilities and network resilience. The logic of this action assumes that if there are no vulnerabilities for exploitation then there is no cyber attack. Secondly, if U.S. cyber assets should fail in denying an adversary the capability to attack, the United States will use the whole-of-government to respond to aggression militarily within cyberspace or within the traditional domains. [28]

This proposed U.S. approach to adversary cyber operations and attack, deterance by committing to all out warfare, may not seem analogous to Douhet's advocated use of offensive strategic bombardment, but there are similiarities. In fact, one could argue that current U.S. cyber policy, which supports a whole-of-government all out war deterrence model, is an updated version of offensive strategic bombardment and pre-emptive strike aimed at shattering civilian morale. By balancing the non-kinetic warfare of cyber attack, meaning no bombs are used, with all out kinetic war leveraging traditional warfare capabilities of land, sea, and air, as is proposed by a whole-of-government approach to war, the United States maintains the focus of shattering civilian morale as a means to deter attack.

Douhet's air doctrine and current U.S. cyber policy both advocate shattering a nation's will to wage war by focusing on degrading civilian support. In Douhet's time through World War II and into Vietnam, strategic bombardment of adversary industrial and logistical capability was an accepted use of air power.

In a modern era of precision munitions and public support decrying collateral damage, strategic bombardment of population centers has been modified, but still retains the goal of diminishing adversary popular support for war. In the modern era popular

[28] Ibid., 2.

uprising often can overthrow a government. Proposing all out war, and pursuing actions against the United States which has demonstrated the capability to conduct sustained warfare, proves to be a powerful deterrent that can cause potential adversaries to take pause.

Along with Douhet's push for pre-emptive strategic bombardment as a means to deter warfare, American air power theorist William Mitchell argued for a dedicated service to ensure air power was a dominant warfare capability. [29] Mitchell's advocacy for a highly skilled and trained air force during the 1920s and 1930s is similar to the push for a similarly technically sound cyber force. This also makes logical sense due to the very technical nature and specialized support structure needed to both maintain aircraft as well as computer systems and networks.

Building off what seems technically sound, the U.S. military saw the creation of both an Air Force, in 1947, and Cyber Command, in 2009, to deal with the technical intricacies of conducting warfare in new areas as well as codifying the doctrinal dogma that guides these operations. The mapping of air power and cyber power development, which focuses on meeting capability with defense is almost analogous; however this mapping does not necessarily support that cyberspace is indeed an operational domain.

There remain key discrepancies between air power and cyber power that may support the conclusion that cyberspace is not an operational domain but an enabling function for pre-existing domains such as aerospace, land, and sea.

Power projection has been key to the codifying of aerospace as an operational domain. This power projection is grounded in attribution and proven demonstration of

[29] Op. Cit., Edward Warner, 485.

capability during war. The anonymity of cyber power and lack of public and attributable U.S. demonstration of cyber capabilities greatly impacts the notion that cyberspace is an operational domain as compared to land, sea, air, and space. Unlike cyberspace, the U.S. has proven capability time and again in the physical domains. This leads to the conclusion that the virtual domain of cyberspace is not an operational domain analogous to land, sea, air, and space.

Discussion & Implications

The growth of aerospace as an operational domain and the subsequent development of air power have followed a progression of capability which can be simplified in terms of offense and defense in the context of capability and deterrence. To map out the development of air power, aircrafts were first used as reconnaissance in warfare. Adversaries met reconnaissance by developing anti-aircraft artillery (AAA). Anti-aircraft artillery led to the development of armed aircraft with attack capabilities, to protect and deter AAA. Armed aircraft resulted in aircraft to aircraft aerial fighting. All of these capabilities were developed during WWI. The true strategic bombardment capabilities advocated by Duet did not come to fruition until World War II, almost a generation after air power was first used operationally, due to limits in technologic capability to support sustained flight and the carrying of large loads of munitions during WWI. In this case doctrine and theory, which was eventually proven sound, outpaced capability.

Douhet's vision of a true aerial strategic deterrent was not fully realized until 1945, when long-range aerial bombardment was married with the atomic bomb. This was fifteen years after Douhet's death and twenty-four years after he first advocated strategic

bombardment in his treatise *The Command of the Air*. In this case theory and doctrine outpaced technology. The atomic age, and fully realized aerial strategic bombardment helped to usher in Mitchell's dedicated Air Force (if only to maintain and ensure the first side of the nuclear triad). In all, it took a generation for the air warfare theory and doctrine developed during the 1920s and 1930s to be fully realized into air power.

In comparison we see have seen a limited, but similar progression of cyber doctrine and demonstration potential for cyber conflict and warfare although no proven and attributable use of cyber power. The nuance between conflict and warfare is one of degrees of nuisance and destruction. Cyber conflict has been defined as the use of cyberspace to attack, defend, and spy on one another "for political or other national security purposed" to the point of not causing destruction that would mirror the effects caused by traditional kinetic military attack. [30] The preponderance of publicly known cyber related incidences have been within the spectrum of conflict and not attack, and have been greatly focused on spying and acts of espionage to include the theft of intellectual property aimed at providing economic and technologic advantage. A majority of the targets for this conflict have been military.

The United States recognizes defensive aspects of cyber security "as one of the most serious economic and national security challenges," while conceding further that the United States is not prepared to counter the current threat. [31] The U.S. military's "global communications backbone… consists of 15,000 networks and seven million computing

---

[30] Healey., 15.

[31] Executive Office of the President of the United States of America, "The Comprehensive National Cybersecurity Initiative," accessed November 11, 2013, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

devices across hundreds of installations in dozens of countries." [32] This extensive information technology infrastructure, which does not include private industry that supports the military or broader government, facilitates U.S. military command and control but also logistical support, real-time provision of intelligence to forward forces in austere environments, and general communications. [33] The U.S. military, government, and economy are reliant on cyberspace, the Internet, and related IT for a preponderance of day-to-day functions. Dependency without redundancy leads to risk. The United States' over reliance on cyberspace and the Internet is hazardous, as shown by a breakdown in control over Department of Defense networks in 2008.

The U.S. Department of Defense (DoD) suffered "the most significant breach of U.S. military computers ever" in 2008. [34] This compromise, coined Operation Buckshot Yankee, was perpetrated by a foreign intelligence service through an infected laptop at U.S. Central Command, based in the Middle East. The state perpetrator has not been made public.

Buckshot Yankee, which was initially introduced to a U.S. laptop from USB flash drive, quickly replicated itself on both classified and unclassified military government computers.[35] This malicious software (malware) allowed data to be transferred without the U.S. government's knowledge to the foreign intelligence service that created it. I t is currently unreported how many military secrets and how much information was compromised due to this cyber espionage; however, one can be certain

[32] Lynn, "Defending a New Domain," 98.

[33] Ibid., 98.

[34] Ibid., 97.

[35] Ibid., 97.

that this information, whatever it is, is now being used to gain advantage over the United States. Cyber espionage, a small segment of the cyber spectrum of conflict, like Buckshot Yankee, erodes U.S. military effectiveness.

In response to the Buckshot Yankee intrusion, the U.S. military implemented new defensive protocol and security rules for transferring data between networks.[36] These procedures have helped to mitigate the vulnerabilities associated with introducing outside hardware and software to secure networks; however, reactionary responses, such as these, do not eliminate the threat, especially since these protocols were only enacted on government networks, and not the vast networks of the civilian sector that supports the government.

U.S. military and civilian networks are probed and scanned for software and hardware vulnerabilities millions of times per day, as former U.S. Deputy Secretary of Defense, William J. Lynn III, notes.[37] With the ever-growing complexity, size, and dependency the United States places on its information technology, the Internet, and cyberspace, there are bound to be weaknesses that adversaries can exploit. In short, determined actors, if they find vulnerability, can "threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target."[38]

The anonymity associated with perpetrating acts associated with cyber conflict is one of the key factors in making it difficult to label cyber space as an operational domain.

---

[36] National Security Agency, (briefing presented at the 2012 Intelligence Support to Cyber Conference, Ft. Meade, Maryland, U.S.A, July 10-12, 2012).

[37] Lynn, "Defending a New Domain," 97.

[38] Ibid., 99.

Although cyber power's progression maps well with the progression of air power as highlighted by the tit for tat between offensive and defensive capability creation, the lack of attribution of capability is a hindrance to cyber space being labeled as an operational domain, and leads to the conclusion that cyberspace is a an enabling environment in virtual reality to support and reinforce national security in the traditional physical domains of land, sea, air, and space.

The implications of this conclusion are not damning to the supporting effect cyberspace and cyber capability can provide to national security. This conclusion implies that government and national security should consider cyberspace a tool and an enabler to support joint warfare that leverages the whole of government. In the context of the Napoleonic concept of total war, which modern warfare finds significant roots, cyber conflict becomes a key enabler and global commons to exploit to achieve national security initiatives.

The proponents for air power and the creation of a distinct service element to command it initially thought that aircraft could win a war and that armies and navies would become obsolete. As air power theory has evolved this notion has changed. The domain of aerospace and its associated air power are now seen as distinct capabilities to support joint operations, as seen in the concepts of air support to ground operations and airlift associated logistics.

The idea of cyberspace as an operational domain may change in the coming years. At this time, there have been no attributed demonstrations of cyber power as a key-deciding factor in conflict. This may change. One could think of scenarios that would meet a threshold of strategic surprise, a cyber Pearl Harbor if you will. In this case, if

cyber power was to become a deciding factor in conflict, which means it would be proven in conflict and attributable to a state, it could be argued that cyberspace is an operational domain akin to land, sea, air, and space.

Summary Evaluation of Hypothesis One

Contrary to U.S. doctrine and global military thought, cyberspace is not an operational domain akin to land, sea, air, and space. The manmade nature of cyberspace compounded by the fact that cyber power has not been found proven, attributable, or decisive in conflict supports this conclusion.

The future of cyber power and cyberspace is still to be determined. If cyber power becomes a deciding factor in future conflict, it may meet the threshold of becoming an operational domain; however, the fact that cyberspace effects manifest themselves in the physical realities of land, sea, air, and space remains a barrier to it becoming a distinct domain.

Cyber effects may one day prove to be pivotal as the world becomes increasingly interconnected through its networks. This increase in global interconnectivity and dependency opens up areas of study looking into the implications of cyberspace as global commons. As cyberspace and the Internet proliferate global life, should cyberspace become protected under international law? Will cyberspace become so critical to future commerce and society that it is granted the same protections that international waters and space have to ensure that they remain accessible to all peoples?

Bell's telephone changed how humanity was able to communicate and interact, becoming adapted and integral to modern military command and control. In spite of this, the telephone has never been thought of as a unique domain of warfare. Cyberspace for

all its life changing impacts, and initial foundation of Bell's telephone lines, remains similarly bound; at this time cyberspace is not a distinct operational domain of warfare, but an enabler.

CHAPTER 3: AN EXAMINATION OF IMPEDIMENTS TO U.S. TECHNICAL RECRUITMENT OF CYBER WARRIORS

As discussed in chapter two cyberspace is an artificial reality resident and routed through an ever-growing global network of software and hardware, computers and information technology, that is increasingly connecting the developed and developing world. The U.S. Department of Defense (DoD) has labeled cyberspace as the latest operational domain of warfare, akin to the traditional domains of war, land, sea, air, and space, a topic previously explored and refuted. [39]

Coinciding with this status elevation, the DoD has increasingly invested in its cadre of cyber professionals, since Deputy Secretary of Defense William Lynn III released the 2011 *Department of Defense Strategy for Operating in Cyberspace*. [40] The July 2011 strategy outlined five strategic initiatives:

> (1) Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential
>
> (2) Employ new defense operating concepts to protect DoD networks and systems
>
> (3) Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy
>
> (4) Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity
>
> (5) Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

[39] *Department of Defense Strategy for Operating in Cyberspace*, Washington, DC: U.S. Department of Defense, 2011., 5.

[40] Ibid.

To help meet these initiatives the annual portion of the DoD budget dedicated to cyberspace has increased by almost $1 billion annually from 2013 to 2015. [41] [42] Although only one percent of the overall defense budget, the 2015 cyber budget is estimated to be $5.1 billion. [43] This three year budgetary increase has included an over 8,000 person plus up in the cyber workforce of the U.S. Department of Defense. [44]

The DoD's cyber workforce includes personnel working for the various services, Army, Air Force, Navy, and Marines, as well as the National Security Agency (NSA) and joint combatant command U.S. Cyber Command (also known as CYBERCOM). [45] As the U.S. DoD has solidified their strategic vision for cyberspace they have levied an increasing demand single on recruitment, retention, and training of highly technical and specialized cyber experts. The DoD has begun calling this cadre of military cyber professional cyber warriors. This term is often used when describing the uniformed military members serving in the various branches of the U.S. Armed Services, but has also been used to describe the civilian defense personnel supporting the department's cyber mission.

So who are these cyber warriors? Where do they come from, and how does one become join the ranks? These two questions, in the context of the *Department of Defense*

---

[41] Kevin McCaney, "DOD budget reflects impact of cyber, unmanned systems, R&D," *Defense Systems*, March 4, 2014, Accessed October 10, 2014, http://defensesystems.com/articles/2014/03/04/dod-2015-budget-technology.aspx.

[42] Brendan McGarry, "NSA Chief: What Cyberwarrior Shortage?" *Defenstech*, October 14, 2013, Accessed October 10, 2014, http://defensetech.org/2013/10/14/nsa-chief-what-cyberwarrior-shortage/ .

[43] Ibid.

[44] Op. Cit., McCaney, "DOD budget reflects impact of cyber, unmanned systems, R&D."

[45] Op. Cit., McGarry, "NSA Chief: What Cyberwarrior Shortage?"

Strategy for Operating in Cyberspace fifth strategic initiative (leverage the nation for a cyber workforce), formed the basis of an examination of the U.S. Department of Defense's most basic pipeline for recruitment, college and university graduates of Computer and Information Science programs.

Literature Review

There is little currently written on what constitutes a cyber warrior in the realm of national defense or more specifically the U.S. Department of Defense. In order to examine this area for evidence or information that is part of the current state of literature this study reviewed press releases, education statistics for the computer and information science degree paths, as well as recruitment and military demographics of the personnel pools from which cyber warriors or experts would be selected within the active duty component of the U.S. Department of Defense.

Israel recently announced that it was moving to allow its defense related cyber experts to network and share ideas with private sector Israeli industry as a means to spur innovation. [46] Additionally, Israel recognizes that its cyber military cadre are distinctly different from its traditional compulsory military force, noting that its best cyber capability comes from individuals who do not adhere to the traditional military lifestyle of discipline and taking orders. [47] The idea of military recruitment and the impact of voluntary and compulsory service on the inclusion of technical expertise with national

[46] William Booth and Ruth Eglash, "Young Israeli cyberwarriors learn to duel in the dark," The Washington Post, October 8, 2014. Accessed October 12, 2014, http://www.washingtonpost.com/world/young-israeli-cyberwarriors-learn-to-duel-in-the-dark/2014/10/07/e07a9031-1e01-4815-8938-5fab87495e82_story.html.

[47] Ibid.

military's may be a topic for further research, but is outside the scope of this analysis which focuses upon the U.S. DoD's cyber warriors.

Israel and Great Britain are also leveraging untraditional areas for recruitments of their cyber work force. Each nation is engaging with pre-collegiate groups through competitive hacking initiatives offering prizes of scholarships and jobs to the winners. This type of recruitment is embracing the non-traditional roots of hacking, and cyberspace exploitation that is learned through hands-on experience not education programs. [48] An area for additional research that could possibly add to this review would be an examination of the hacker culture of cyberspace and how one becomes a hacker. A better understanding of hacker conventions which sponsor and discuss ethical hacking, may be a starting point for this research.

Methodology & Hypothesis

As previously discussed the U.S. Department of Defense (DoD) has both civilian and uniformed (traditional military) cyber warriors in its workforce. As outlined in the literature review, education and training in computer and information science as well as computer security certifications are traditionally the driving factors, which qualify civilians to pursue a career working in cyberspace (be it programming, developing, or architecting computers and networks) supporting private and public sectors.

The culmination of exploring the current literature dealing with cyber expertise resulted in asking the following question: How does the U.S. Department of Defense

[48] Bloomberg Businessweek, "How a Spy Agency Recruits Future Cyber Warriors," *Bloomberg Businessweek Videos*, 2:00, March, 17, 2014, http://www.businessweek.com/videos/2014-03-17/how-a-spy-agency-recruits-future-cyber-warriors .

compete with the private sector in the recruitment of the technical expertise needed to develop cyber warriors?

In order to answer this question, the following analysis will attempt to tease out the different cyber career and education paths for U.S. Department of Defense civilians and active duty military personnel, comparing and contrasting how these two groups are trained to become cyber warriors. It is hoped that in comparing and contrasting the paths, that the analysis will identify similarities and differences that may help to answer how well the DoD is competing with private industry in the recruitment and grooming of the highly technical skills associated with cyberspace. Additionally, by answering how well the DoD is competing with private industry recruitment, this analysis may identify opportunities or areas that could benefit from additional analysis, support, or research.

Data & Results

This study focused on analyzing the major sources of recruits for military civilian and active duty enlisted personnel who would fill roles as cyber warriors as a means to compare and contrast the sources to highlight disparities and possible areas for improvement. Firstly, table two below, outlines the minimum age requirements for each U.S. military service. As a general rule of thumb, it is very difficult to enter initial active duty military service beyond the age of thirty-five. In 2012, 48.8 percent of the active duty enlisted military force was twenty-five years of age or younger, and 23 percent of the force was between the ages of twenty-six and thirty. [49] In total, almost 72 percent of the force was aged thirty years or younger. Additionally, only 5.9 percent of the total

[49] Department of Defense, United States of America. *2012 Demographics Profile of the Military Community*, Department of Defense, 2012, Accessed November 4, 2014, http://www.militaryonesource.mil/12038/MOS/Reports/2012_Demographics_Report.pdf.

active duty enlisted force has a bachelor's degree or higher. These statistics highlight that the majority of the resource pool that the military is pulling from in order to fill its ranks, including its cyber warriors, has little to know formal education beyond the requisite high school level.

To help mitigate this lack of formal post-secondary education, the military has created and instituted training for its cyber warriors that is almost seven months long. [50] This research was unable to locate or identify the curricula that constitutes this training for comparison to traditional public education within the computer and information science fields, and highlights an area for possible future research.

To join the...	Age
Air Force	17-27
Army	17-34
Coast Guard	17-39
Marines	17-29
Navy	17-34

Table 2. U.S. Armed Services' Enlistment Age and Dependent Requirements [51]

As an aside, figure 1, below, depicts military recruitments nationally per one thousand youths, and highlights that traditional urban areas, to include Silicon Valley, are under represented in recruitment. Although not coincidental and not conclusive, there may be valuable information gleaned from future analysis of military recruitments with specific area education standards including Internet and computer education courses. This

[50] Sternstin, Aliya. "Qualifying Cyber Command Staff is Harder Than You Think," *Nextgov*, April 14, 2014, Accessed October 10, 2014, http://www.nextgov.com/cybersecurity/2014/04/cyber-warrior-training-no-easy-task/82498/

[51] Military.com, "Are You Eligible to Join the Military?" *Military.com,* Accessed November 4, 2014, http://www.military.com/join-armed-forces/join-the-military-basic-eligibility.html

analysis may highlight that the military's recruitment is not targeting the proper demographic to meet the specific introductory technical skills required for a cyber work force resulting in the need for additional training efforts and education cost to the military.

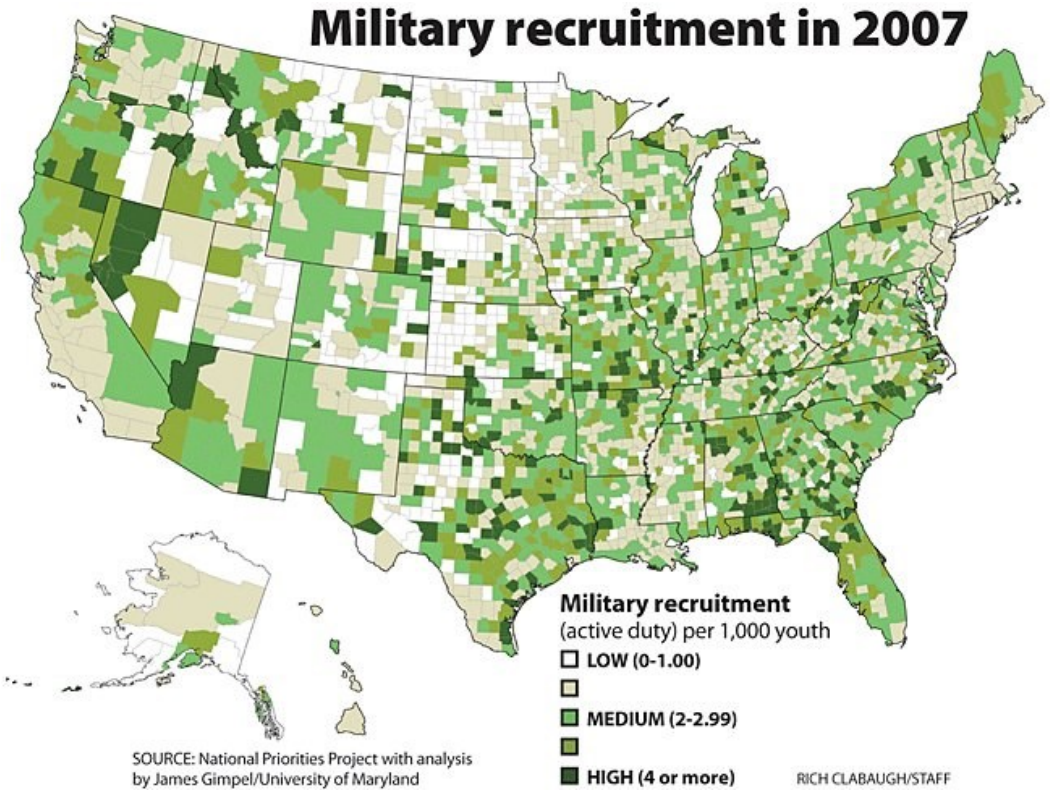

Figure 1. Military recruitment nationally per 1,000 youth

Unlike the DoD's enlisted pool of potential cyber warriors, who have little specialized secondary training in computer or information science, and require abridged military training lasting approximately seven months with an unknown amount of on the job training, the civilian pool of candidates to draw cyber expertise from traditionally has post-secondary education.

As a percentage of all U.S. bachelor degrees conferred, degrees in Computer and Information Science (the traditional discipline to equip cyber expertise) has routinely been under represented. Since 1979 this degree field has accounted for no more than 4.5 percent of all degrees conferred, and most recently has accounted for only 2.6 percent of the total 1,791,046 bachelor degrees earned in 2012, a mere 47,384 degrees (Figures 2 and 3). [52] The number of private sector jobs supporting cyberspace (computer programmers and computer systems analysts) numbered 864,300 in 2012; these jobs are forecasted to grow to over one million by 2022, a 16 percent increase. [53] [54]

[52] National Center for Education Statistics, "Bachelor's degrees conferred by postsecondary institutions, by field of study: Selected years, 1970-71 through 2011-12," *Digest of Education Statistics*. Accessed October 12, 2014, http://nces.ed.gov/programs/digest/d13/tables/dt13_322.10.asp .

[53] Department of Labor, United State of America, "National Employment Matrix for Computer Programmers," *Bureau of Labor Statistics*, Accessed November 4, 2014, http://data.bls.gov/projections/nationalMatrix?queryParams=15-1131-143&ioType=o .

[54] Department of Labor, United State of America. "National Employment Matrix for Computer Systems Analysts," *Bureau of Labor Statistics*, Accessed November 4, 2014, http://data.bls.gov/projections/nationalMatrix?queryParams=15-1121-145&ioType=o .

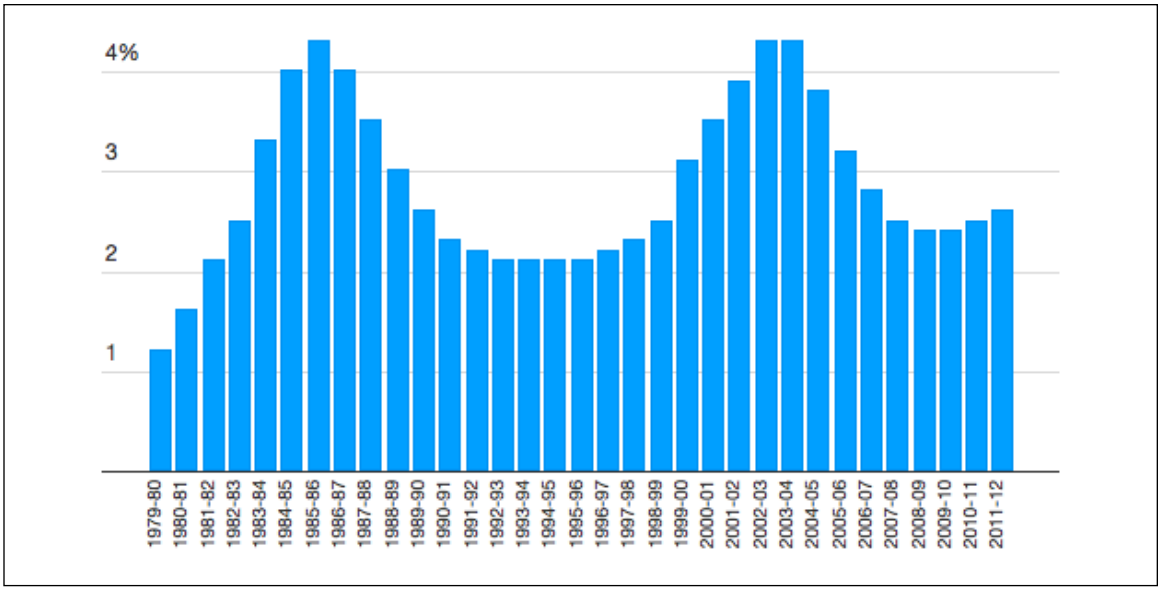

Figure 2. U.S. Computer and Information Science degrees conferred from 1979 to 2012 as a percent of all bachelor's degrees [55]

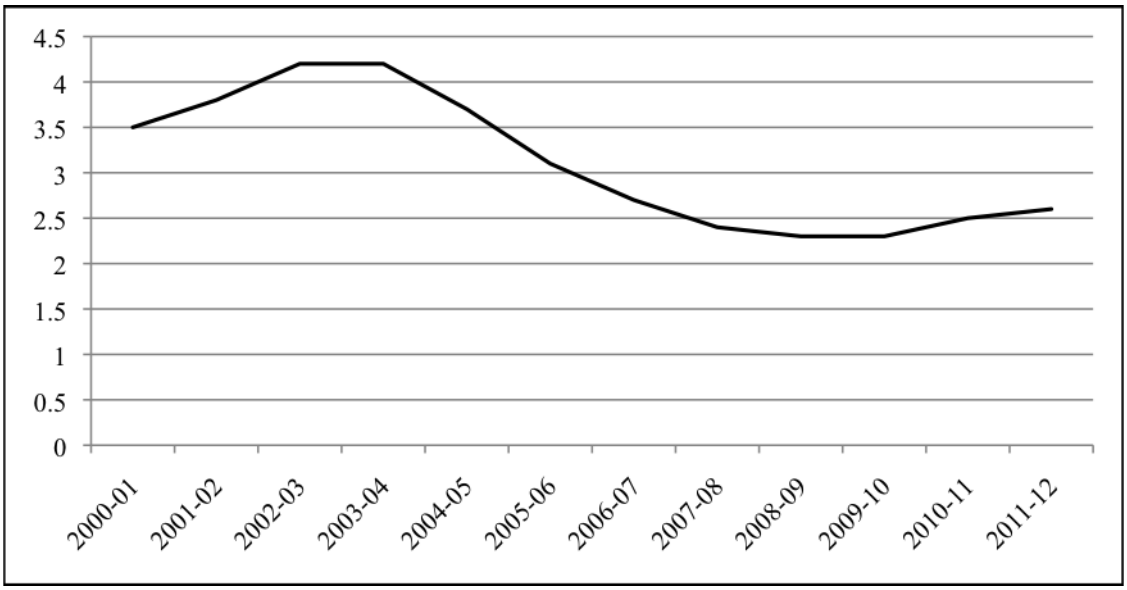

Figure 3. Total U.S. Computer and Information Science degrees conferred at the bachelor's level from 2000 to 2012 as a percent of all degrees [56]

[55] Jonah Newman, "Is There a Crisis in Computer-Science Education," *The Chronicle of Higher Education*, June 23, 2014, Accessed October 9, 2014, http://chronicle.com/blogs/data/2014/06/23/is-there-a-crisis-in-computer-science-education/.

[56] National Center for Education Statistics, "Bachelor's degrees conferred by postsecondary institutions, by field of study: Selected years, 1970-71 through 2011-12," *Digest of Education Statistics*. Accessed October 12, 2014, http://nces.ed.gov/programs/digest/d13/tables/dt13_322.10.asp .

The U.S. colleges and universities have graduated less than 60,000 students in the Computer and Information Science fields annually since 2000 (Figure 4). Of these graduates, women graduates count for on average less than a third of all bachelor's degrees awarded, and equally if not worse percentage of master's and doctorate degrees awarded (Figures 4, 5, and 6). These graduations, which are a fraction of all U.S. graduations, highlight a significant lack of diversity in the fields that cyber warriors will be derived from, and may serve as an impediment to the Obama Administration's and Department of Defense's push for a diverse workforce as outlined in Executive Order 13581 and the *DoD's Diversity and Inclusion Strategic Plan for 2012 - 2017*. EO 13581 "directs executive departments and agencies to develop and implement a more comprehensive, integrated, and strategic focus on diversity and inclusion as a key component of their human resource strategies. While EO 13583 was focused on civilian personnel, this Strategic Plan also addresses similar concerns for military personnel." [57]

---

[57] Department of Defense, United States of America, *Department of Defense Diversity and Inclusion Strategic Plan 2012- 2017*, Department of Defense, 2012. Accessed October 10, 2014, http://diversity.defense.gov/Portals/51/Documents/DoD_Diversity_Strategic_Plan_%20final_as%20of%2019%20Apr%2012[1].pdf .

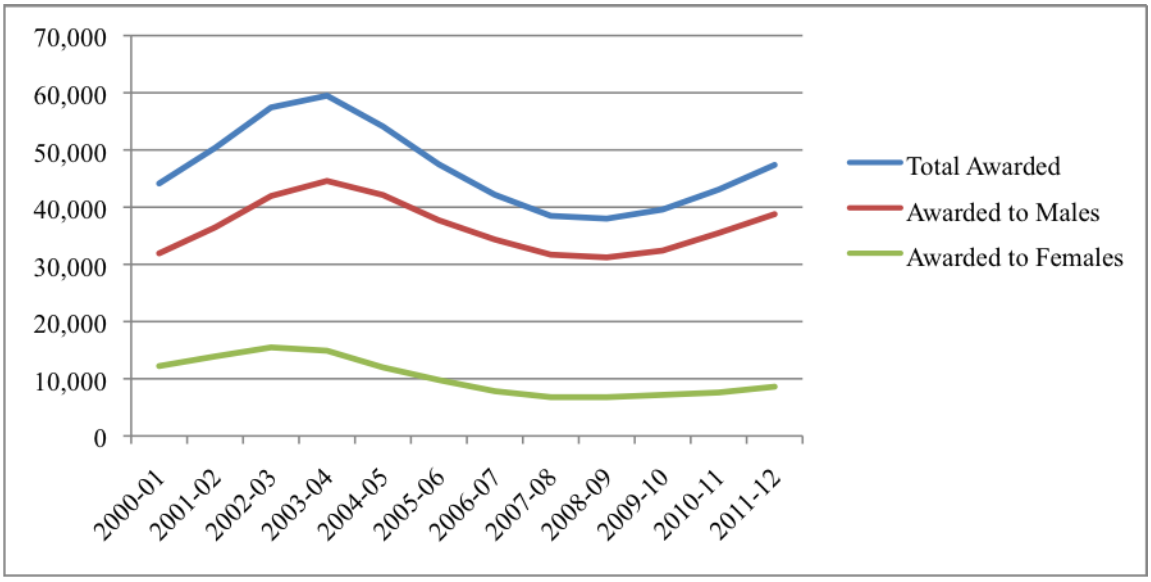

Figure 4. Total number of U.S. Computer and Information Science degrees conferred at the bachelor's level by gender from 2000 to 2012 [58]

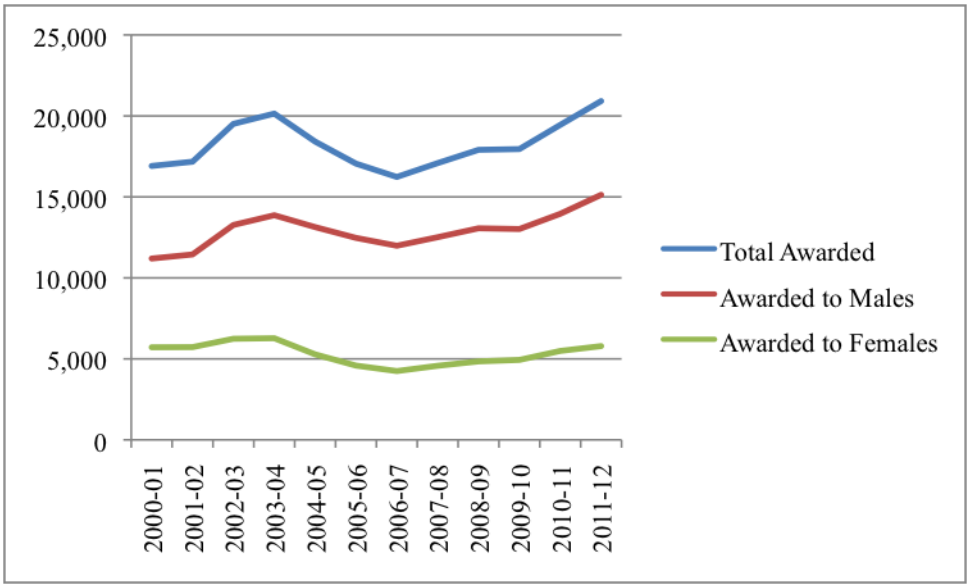

Figure 5. Total number of U.S. Computer and Information Science degrees conferred at the master's level by gender from 2000 to 2012 [59]

[58] National Center for Education Statistics. "Degrees in computer and information sciences conferred by degree-granting institutions, by level of degree and sex of student: 1970-71 through 2010-11." *Digest of Education Statistics*. Accessed October 12, 2014. http://nces.ed.gov/programs/digest/d12/tables/dt12_349.asp

[59] Ibid.

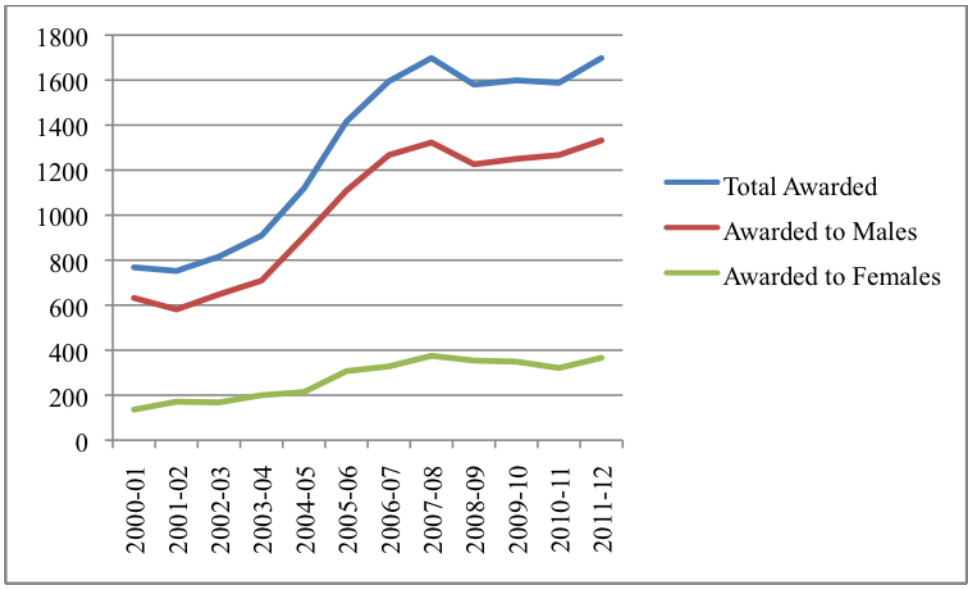

Figure 6. Total number of U.S. Computer and Information Science degrees conferred at the doctorate level by gender from 2000 to 2012 [60]

Discussion & Implications

There are major implications with the recruitment of Department of Defense cyber warriors for active duty service as well as civilian positions. As previously discussed, the main impediment for recruiting cyber expertise for the active duty military is the fact that so little of the enlisted work force has higher education or technical skills which would be learned in higher education. This results on the onus of the education and training being carried by the DoD and military service components, in short then military has to complete 100 percent of the cyber training and education of its uniformed workforce; a major investment. An additional impediment for the recruitment of cyber expertise within the uniformed military may be as simple as the traditional height, weight, and fitness standards the military adheres to. The U.S. Army has recently begun

[60] Ibid.

investigating the relaxation of their physical fitness requirements for those technical fields, such as cyber warriors. [61] Relaxing these restrictions, along with those of age, may help the military attract individuals who have spent years in post secondary education, honing their understanding of cyberspace; a demographic that may have been traditionally overlooked as they push the uniformed active duty enlisted military age limits with advanced degrees and perhaps less than peak physical standards.

Perhaps one of the most glaring aspects of the recruitments of a diverse civilian workforce is the current disparity in the number of males and females who pursue degrees, both basic and advanced, within the Computer and Information Science fields, as highlighted previously. Beyond the fact that few women pursue masters or doctoral degrees in this field, there are a limited number of these degrees conferred as a whole each year as a percentage of all degrees. Will this limited enrollment, of which only less than 3 percent of all bachelors are now pursued annually in the last decade, create enough of an educated pool of candidates to meet both public and private sector demands? With total number of private sector jobs forecasted to exceed one million by 2022, it may become increasingly difficult for the government and DoD to recruit and retain such a specialized workforce, unless compensation increases (an area which could use more research and study to determine the optimal compensation to compete with private sector).

[61] Christian Datoc, "The (Not So) Thin Red Line: Army Set To Change Phys. Requirements For 'Cyber Warriors'." *The Daily Caller*, October 28, 2014, Accessed November 4, 2014, http://dailycaller.com/2014/10/28/the-not-so-thin-red-line-army-set-to-change-phys-requirements-for-cyber-warriors/ .

One aspect of this research that is lacking is a better understanding of the number of U.S. degrees granted to non-citizens. As most Department of Defense and government positions require U.S. citizenship in order to obtain a security clearance, that actual pool of candidates eligible to work for the DoD and government out of the total that have degrees may be far less. This data was not available from the National Centre of Educational Statistics at the time of this works completion, and identifies an area for future research.

Summary Evaluation of Hypothesis Two

CHAPTER 4: CHINESE MOTIVATIONS FOR CYBER-ENABLED INTELLECTUAL PROPERTY THEFT

The United States is the world leader in technology innovation and intellectual property (IP) creation. In calendar year 2013, the United States led the world in patent creation, accounting for 48.7 percent of all patents granted (147,652 of 302,948).[62] U.S. intellectual property creation continuously spurs economic development, contributing to manufacturing which on average accounts for over $2 trillion of the U.S. national economy (about 12 percent of GDP).[63]

Since its late 20th Century commercial popularization and adoption by industry, the Internet has increasingly served as a major access point for global information and knowledge distribution. In 1993 the Internet accounted for 1 percent of globally telecommunicated information; today, the Internet accounts for more than 97 percent of all telecommunicated information worldwide.[64] U.S. "energy, banking and finance, transportation, communication, and … Defense Industrial Base" sectors are connected to the global economy via the Internet.[65] The rapidity of Internet based communication and knowledge dissemination has no doubt contributed to economic globalization and the growth of U.S. industry. Although U.S. industry has prospered from the connectedness

---

[62] United States Patent and Trademark Office, "Patent Counts by Origin and Type Calendar Year 2013," http://www.uspto.gov/web/offices/ac/ido/oeip/taf/st_co_13.htm.

[63] National Association of Manufacturers, "Facts About Manufacturing in the United States," Accessed July 10, 2014. http://www.nam.org/Statistics-And-Data/Facts-About-Manufacturing/Landing.aspx

[64] Hilbert, Martin and Priscila López, "The World's Technological Capacity to Store, Communicate, and Compute Information," Science, 2011, 332(6025), 60–65.

[65] Department of Defense, United States of America. *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://www.defense.gov/news/d20110714cyber.pdf.

of the Internet, high technology business areas have become increasingly vulnerable to exploitation via Internet enabled intellectual property theft by state and non-state actors.

At least half a dozen countries are currently exploiting U.S. corporate and military computer systems via the Internet and cyberspace to gain both economic and military advantage.[66] The People's Republic of China (PRC) and more specifically the People's Liberation Army (PLA) 3rd Department of the General Staff, also known as Unit 61398, has come to light in recent press reporting as a prolific actor in the realm of Chinese cyber espionage and intellectual property theft.[67] The PLA's efforts to exploit U.S. high-tech industry via cyber has been known to the U.S. government for many years; however, substantial knowledge of these efforts have just recently (2011 to current) become available to the general public.

It is difficult to estimate the true cost of cyber exploitation, as there are no international, federal, or state mandates to report cyber incursions or theft. Intellectual property theft via cyber exploitation can be swift, going unnoticed or even unreported. For example, "$1 billion – 10 years' worth of research and development" was lost by one U.S. Company in a weekend after being attacked, and it is reported that the United States, across all industries, loses between $6 billion and $20 billion annually in intellectual property and investment opportunities.[68]

---

[66] Ellen Nakashima, "Several nations trying to penetrate U.S. cyber-networks, says ex-FBI official," Washington Post, April 18, 2012, available at http://www.washingtonpost.com/world/national-security/several-nations-trying-to-penetrate-us-cyber-networks-says-ex-fbi-official/2012/04/17/gIQAFAGUPT_story.html.

[67] Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*, February 2013, accessed May 4, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[68] Nakashima, "Several nations..."

Cyber exploitation and intellectual property theft directly undermines the United States government, its business, and industrial base, while simultaneously posing a significant threat to the nation's long term "military effectiveness and its competitiveness in the global economy."[69]

The PRC vehemently denies that it is exploiting U.S. interests in cyber space.[70] China's denials of intellectual property theft via the Internet and cyber-enabled exploitation, in spite of contrary reporting, is intriguing and calls for further investigation.

This study will aim to discover the motivation for the People's Republic of China's military targeting of U.S. intellectual property (IP) by cyber-enabled theft and espionage. The following analysis will compare and contrast China's strategic goals and objectives, as outlined in the nation's Five-Year Plans, with China's military doctrine and motivation. It is hoped that any strategic correlations in objectives and doctrine will be able to be linked with real world examples of cyber theft and espionage as a means to verify these relationships.

By identifying and verifying the PRC's motivations for cyber-enabled IP theft and economic espionage, it may possible to determine the key industrial areas the PRC will target and exploit in the future. By simply monitoring the open communication of the PRC's Five-Year Plans the U.S. may be able to develop key recommendation to U.S. industry of sectors that will require additional cyber protection and hardening. If this

---

[69] William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, vol. 89, no. 5 (September/October 2010), 100.

[70] Xu Weiwei, "China denies hacking claims." February 20, 2013, accessed May 5, 2013, http://www.morningwhistle.com/html/2013/PoliticsSociety_0220/217214.html.

analysis proves successful it will help to provide a mechanism of warning, which may allow a competitive advantage for protection of communication and cyber infrastructure against Chinese exploitation.

Literature Review

Since 1993, China's military leadership has embraced the concept that cyberspace is a key warfare domain that must be controlled in order to maintain warfare effectiveness in air, sea, and space conflicts.[71] [72] China's strategic military motivations for embracing cyberspace as a warfare domain is the most recent addition to a holistic national strategy aimed at increasing China's economic development and independence.[73] China's 7th Five-Year plan, announced in 1986, announced the PRC's strategic goal to increase its economic prosperity through economic development.[74] As a means to further refine and center China's whole of government economic development efforts, the People's Republic created the 863 Program.[75] [76]

---

[71] The Central Military Commission (CMC) revised the PLA's Military Strategic Guidelines in 1993 under Jiang Zemin stating that the PLA should prepare to "fight local wars under high-tech conditions." See Krekel pp 14.

[72] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Northrop Grumman Corporation, March 7, 2012, 14.

[73] China.org.cn, "The 7th Five Year Plan (1986-1990), accessed June 21, 2014, http://www.china.org.cn/english/MATERIAL/157620.htm.

[74] Ibid.,

[75] The numbering convention of 863 is derived from the establishment of the program in March of 1986, following the date convention for China that lists year followed by month.

[76] Ministry of Science and Technology of the People's Republic of China, "National High-tech (R&D) Program (863 Program)," accessed July 7, 2014, http://www.most.gov.cn/eng/programmes1/200610/t20061009_36225.htm.

The 863 Program focused the People's Republic on establishing a high-technology industrial base as a means to spur its economic growth. The scope of 863 has grown over the last quarter century, influencing successive five-year plans. The 12th Five-Year plan, spanning 2011 to 2015, is the latest plan to continue China's economic growth, concentrating on developing emerging industries that will strategically support the PRC in cultivating growth of technology exports.[77] The PRC's goal is to achieve a ten percent growth rate in exports of high-tech products ultimately reaching $2.5 trillion in exports by 2015.[78]

In a June 2011 article from the Communist Party *Youth Daily (Qingnian Bao),* authors from the People's Liberation Army (PLA) Academy of Military Science espoused the importance of exploiting cyberspace, stating "the quantity of military intelligence information obtained over the Internet is large, the classification level is high, the information is timely, and the cost is low, intelligence reconnaissance activities that are launched over the Internet are already omnipresent and are extremely difficult to defend against."[79] China's military strategy is a reflection of the PRC's over arching goal for maintaining and growing their economic supremacy. China's goal is partially met by rapidly acquiring superior high-tech industrial manufacturing capability through the theft of intellectual property and high-tech know how. This approach uses the Internet as a

[77] China Briefing. "China Releases 12th Five-Year Plan for Trade in Electromechanical and High-Tech Products," June 7, 2012, accessed June 21, 2014, http://www.china-briefing.com/news/2012/06/07/china-releases-12th-five-year-plan-for-trade-in-electromechanical-and-high-tech-products.html.

[78] Ibid.

[79] Krekel., *Occupying the Information High Ground*, 25.

means to asymmetrically level the technological battlefield with strategic rivals and potential future adversaries.

China's state-sponsored information, intelligence, and intellectual property collection from computer network exploitation (CNE), also known as cyber exploitation, espionage or intrusion, is not only targeting military technology but economic and industrial trade secrets spanning such diverse sectors as chemical engineering, automotive construction, and aerospace, as well.[80] All these sectors factor into China's 12th Five-Year Plan as areas where the state can increase its exports and achieve increasing financial gain.

CNE offers individuals conducting cyber espionage a means to remotely access computers and information technology (IT) around the world, rapidly stealing vast amounts of data with little to no risk of attribution.[81] One of the largest examples of this type of exploitation in recent years has come to be known as *Operation Shady RAT*.

Operation Shady RAT, a 2011 report compiled by Dmitri Alperovitch of McAfee, one of the world's largest computer security firms, highlights the hacking of more than seventy-one corporations and government entities around the world by a single actor using RATs from 2006 to 2011.[82] A RAT, an acronym for remote access tool, allows users to remotely access computers without detection giving individuals free access to

[80] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011,* October 2011, 3-5.

[81] Ibid., 1.

[82] Dmitiri Alperovitch, *Revealed: Operation Shady RAT, 2011*, 1-6.

any information stored on the system. This is but one of the many tools threat actors employ to compromise U.S. military and commercial networks.

During his analysis, Alperovitch was able to discern that forty-two of the seventy-one targeted corporations and government entities exploited were in the United States and represented defense contractors as well as state governments.[83] Although McAfee declined to link *Shady RAT* to an individual actor, many cyber security experts believe China was the perpetrator due to the emphasis on targeting information pertaining to Taiwan, the Olympic organization before the commencement of the 2008 Beijing Games, and material covered by the U.S. Department of Defense Military Critical Technology List (MCTL).[84] The MCTL is a list maintained by the U.S. government that highlights technologies unavailable for export.[85] These technologies both provide the United States with military or economic advantage and cannot be exported to countries deemed hostile or competitive to U.S. interests.

The transfer of wealth we are seeing in the form of stolen intellectual property is unprecedented as noted in *Operation Shady RAT* as well as a February 2013 report published by the company Mandiant. The intellectual property that is being stolen through cyber exploitation represents billions of dollars of invested research and development. If only a "fraction of [this knowledge] is used to build better competing products… the loss represents a massive economic threat not just to individual

---

[83] Ibid., 5.

[84] Julie Tate, "Report on 'Operation Shady RAT' identifies widespread cyber-spying," *Washington Post*, July 29, 2012.

[85] The Military Critical Technology List (MCTL) is a compilation of the technologies the Department of Defense deems critical to maintain U.S. military superiority. The technologies associated with this list are often export controlled. For more information on this subject please refer to the Federation of American Scientists' site http://www.fas.org/irp/threat/mctl98-2/.

companies… but to the entire [country]" through decreased economic growth in high-tech fields.[86]

Simply stated, China is investing and using cyber espionage and cyber network exploitation to obtain information and economic advantage. By stealing technology unavailable for purchase, e.g. MCTL, or unrealistic to develop, i.e. too expensive, China is quickly closing its technology gaps.

Defense experts have hypothesized that China's recent advancements in fifth generation stealth aircraft may be directly linked to cyber exploitation of U.S. defense contractors. As highlighted in Mandiant's 2013 report *APT1: Exposing One of China's Cyber Espionage Units*, we now know that the PLA's cyber unit 61398 is most likely behind such exploitation on behalf of the PRC's military and economic goals.

There are circumstantial links between China's exploitation and theft of key intellectual property from technology-based industries via cyberspace and the PRC's economic development goals outlined in successive Five-Year Plan cycles. To date there has not been a systematic mapping of economic technology development areas identified in the Chinese Five-Year Plans with documented cases of Chinese attributed cyber-enable IP theft or economic espionage.

This study will further analyze Chinese attributed IP theft and the targeted industries. The current discourse of Chinese cyber espionage and intellectual property theft must move beyond the simple explanation that the PRC is pursuing economic development and requires the intellectual capital embodied in U.S. IP in order to do this.

[86] Alperovitch, *Revealed: Operation Shady RAT,* 3.

There other motivations and factors at play. Economic espionage is not new, but state-sponsored economic espionage on an industrial scale, as we have seen within China, is.

Hypothesis & Methodology

There is a significant base of evidence within the public arena discussing China's exploitation of cyberspace as a means to obtain information, intellectual property, and overall decision advantage for economic and political gain. The question is no longer if China is targeting U.S. industry, but why. The following analysis shall aim to answer - How does China's strategic Five-Year Plans drive their exploitation of cyberspace as a tool to equip Chinese industry with economic advantage at the detriment of U.S. industry and interests?

This study will attempt to answer this question by examining attributed PRC use of military enabled economic espionage as a means to obtain economic advantage. The ultimate goal of this analysis is to demonstrate that China's national goals and objectives, as outlined in its Five-Year Plans, are driving the technological areas that the Chinese military targets for cyber theft and espionage.

A major aspect of this study will be a comparison of the 7th through 12th Five-Year Plans, as well as resulting programs of concentration (i.e. 863 Program etc.), as means to identify key industrial and technological areas that China hopes to leverage in order to increase their economic development and competitiveness. It is hoped that by examining the Five-Year Plans, a theme of particular economic interests and technological areas will emerge that can subsequently serve as distinct sectors to look for attributed Chinese cyber theft and espionage. Merely correlating the Five-Year Plan industrial focus areas to attributed Chinese origin cyber exploitation does not prove that

the Chinese government is systematically targeting high-tech sectors for military cyber exploitation. In order to strengthen the hypothesis that the high-tech economic development areas, identified in the Five-Year Plans, are driving Chinese military attributed cyber targeting I will investigate the United States' prosecution of Chinese spies.

By correlating the technology sectors targeted by both traditional and cyber-attributed Chinese espionage with the economic development sectors outlined in China's Five-Year Plans, I hope to strengthen the argument that China's strategic economic interest is driving a whole of government approach to technology acquisition, and that the PLA's cyber exploitation is meant to support economic development. Although not a smoking gun, I hope that by identifying and correlating documented instances of traditional espionage with cyber espionage that a temporal relationship will emerge.

If these correlations are sound there should be a temporal decline in documented traditional espionage and theft as cyber-enabled events increase. The logic is that China should reduce traditional espionage efforts, mitigating the risk of a publicized "spy" trial, in support of the anonymity of cyber exploitation and the ability to conduct these operations from within national boundaries, decreasing the risk of discovery, capture, and prosecution.

Additionally, in context of the Asian Miracle, it may be that China's economic interests will focus on increasing high-tech production and exports as a means to develop national wealth, thus leading to an increased consumer base and overall increased Chinese standard of living. If this analysis supports Chinese targeting of industrial sectors with a focus on production and export of high-tech or defense related material,

assessments of Chinese military, political, and territorial claims may need to be increasingly viewed from an economic perspective.

China's military modernization and technology growth may be indeed indicative of a "peaceful rise," if we are seeing China shift its export model from low profit mass consumer goods production (i.e. clothes, throw away trinkets etc.) to high profit high-tech industrial and defense related material.

Data & Results

Since the onset of Deng Xiaoping's reforms the People's Republic of China has strategically focused on economic growth and expansion. In successive Five-Year Plans, China has focused on establishing the economic foundation necessary to shift its economy from a model based on "excess labor" and manual production to one centered on technological innovation and research and development. [87]

China's 7th Five-Year Plan, 1986 to 1990, and its subsequent 863 Program, China's national high-tech research and development (R&D) program, spurred the People's Republic to pursue domestic economic growth by developing key high-technology industrial areas focused on increasing China's influence in the world arena. [88]

From 1986 to 2005, a time period spanning the 7th through 10th Five-Year Plans, 863 focused China's R&D efforts on key areas. These areas included developing:

1. Technologies for the construction of China's information infrastructure.

[87] David Wertime, "It's Official: China Is Becoming a New Innovation Powerhouse," Foreign Policy, February 6, 2014, Accessed August 1, 2014, http://www.foreignpolicy.com/articles/2014/02/06/its_official_china_is_becoming_a_new_innovation_powerhouse.

[88] Ministry of Science and Technology of the People's Republic of China, "National High-tech (R&D) Program (863 Program)."

2. Biological, agricultural and pharmaceutical technologies to improve the welfare of the Chinese people.

3. New materials and advanced manufacturing technologies to boost industrial competitiveness.

4. Technologies for environmental protection, resources and energy development to serve the sustainable development of our society. [89]

Even today, China continues to rely on "foreign technology, acquisition of key dual-use components, and focused indigenous research and development… to advance…" both military and civilian modernization. [90]

China's national drive has spurred traditional industrial and economic espionage as a means to pursue technological innovation in order to meet national modernization objectives dictated by the Five-Year Plans. Be it the use of spies or individuals with sympathies (racial or monetary) to the People's Republic, China is focused on leveling the technologic playing field with the West.

Since 2006, a period covering the 11th and 12th Five-Year Plans, there have been twenty-nine U.S. indictments for economic and industrial espionage against Chinese nationals, or individuals supporting China's interest (See Figure 7). [91]

[89] Ibid.

[90] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2014*, Office of the Secretary of Defense, 2014, pp 13.

[91] United States Department of Justice, "Press Releases 2006 to 2014," accessed August 01, 2014, http://www.justice.gov/opa/pr/2014/August/.

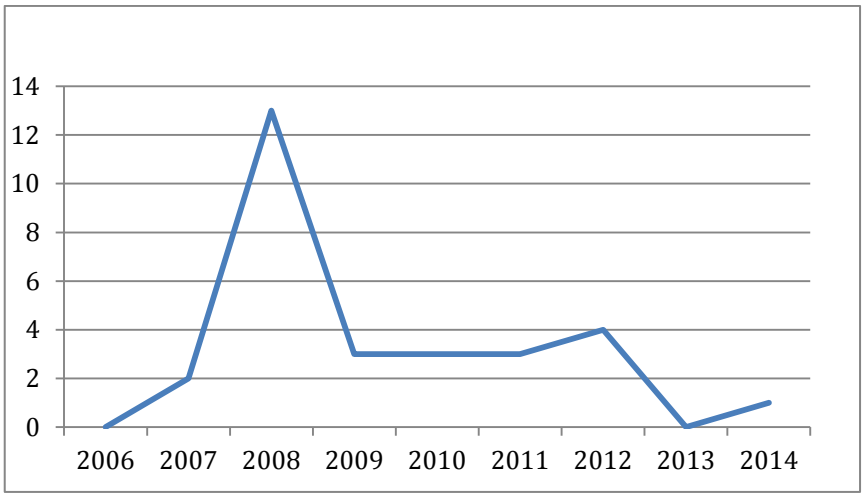

Figure 7. Number of U.S. indictments for Chinese attributed technology espionage since 2006 [92]

The key technologies targeted in these indictments include those industrial areas identified in China's 863 Program (new materials, advanced manufacturing, etc.). [93] As highlighted in Verizon's *2014 Data Breach Investigation Report*, cases of cyber-espionage have risen steadily since 2009 (See Figure 8). [94]

[92] United States Department of Justice, "Press Releases 2006 to 2014."

[93] Ministry of Science and Technology of the People's Republic of China, "National High-tech (R&D) Program (863 Program)."

[94] Verizon, *2014 Data Breach Investigations Report*, Verizon, 2014, http://www.verizonenterprise.com/DBIR/2014/

Figure 8. Cyber breach threat motive over time 2009 to 2013 [95]

In 2013, the United States was the target of more than half (54%) of all cyber-espionage (See Figure 9), followed by South Korea (6%) and Japan (4%). [96] It is rather interesting that the top three nations targeted by cyber-espionage in 2013 are regional peer competitors of the People's Republic.

[95] Ibid.

[96] Ibid.

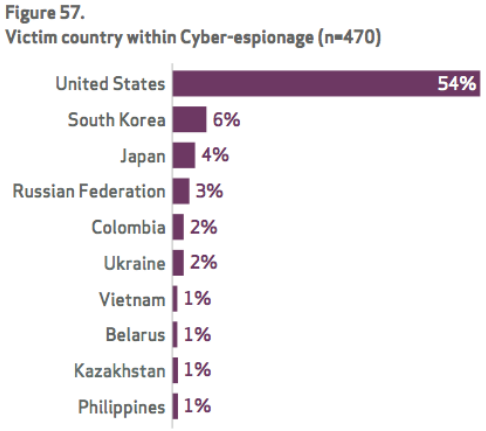

Figure 9. Verizon's 2013 cyber-espionage victim countries by percent [97]

Mandiant's 2013 APT1 report, which attributes known instances of cyber-espionage to Chinese military unit 61398, shows that the preponderance of known Chinese cyber-intrusions have targeted the United States (See Figure 10). [98] Verizon's analysis of regional actors exploiting cyberspace for espionage also highlights Eastern Asia as the point of origin for nearly half of all cyber-espionage in 2013 (See Figure 11). [99] Although not a smoking gun, the fact that in 2013 nearly half of all cyber-espionage originated in Eastern Asia, targeted the United States, and along with China's APT1 focused on the United States as a target, points to China as the likely perpetrator.

[97] Verizon, *2014 Data Breach Investigations Report*, Verizon, 2014, http://www.verizonenterprise.com/DBIR/2014/

[98] Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.*

[99] Verizon, *2014 Data Breach Investigations Report*

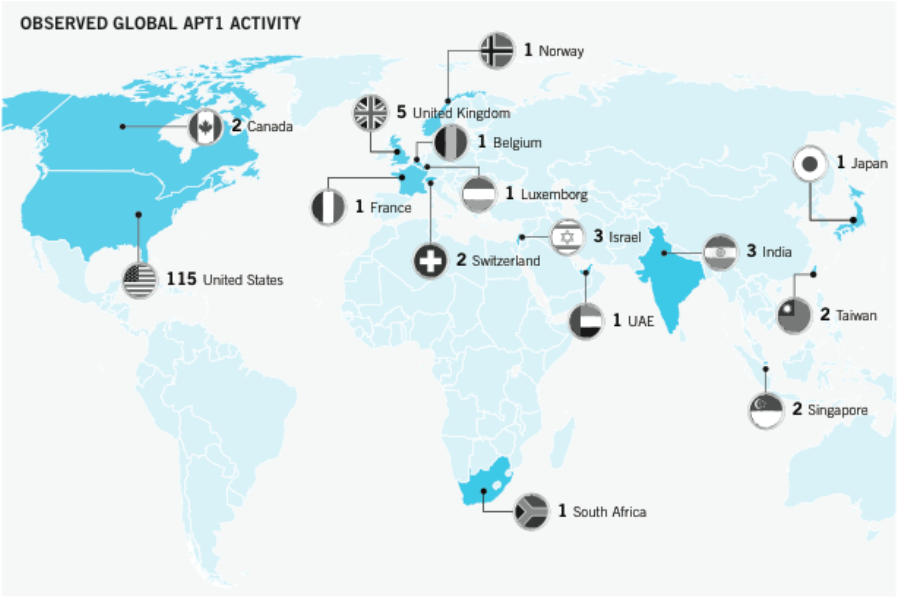

FIGURE 11: Geographic location of APT1's victims. In the case of victims with a multinational presence, the location shown reflects either the branch of the organization that APT1 compromised (when known), or else is the location of the organization's headquarters.

Figure 10. Mandiant's 2013 reporting on Chinese attributed (APT1) cyber-espionage instances by geographic location [100]

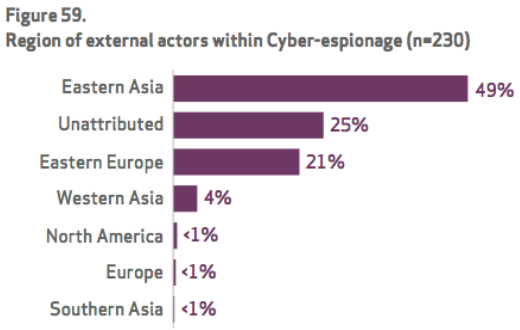

Figure 11. Verizon's 2013 analysis of cyber-espionage actors by region [101]

Furthermore, China's seven priority industries identified in its 12th Five-Year Plan correlate to the industrial areas targeted by China's cyber-espionage unit 61398 (Figures 12 and 13). [102] [103]

[100] Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.*

[101] Verizon, *2014 Data Breach Investigations Report.*

China's 12th Five-Year Plan: Seven Priority Industries	
1	**New energy** • Nuclear, wind and solar power
2	**Energy conservation and environmental protection** • Energy reduction targets
3	**Biotechnology** • Drugs and medical devices
4	**New materials** • Rare earths and high-end semiconductors
5	**New IT** • Broadband networks, internet security infrastructure, network convergence
6	**High-end equipment manufacturing** • Aerospace and telecom equipment
7	**Clean energy vehicles**

Figure 12. China's 12th Fiver-Year Plan Industrial Focus Areas [104]

[102] KPMG, *China's 12th Five-Year Plan Overview*. KPMG, March 2011, http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf.

[103] Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.*

[104] KPMG, *China's 12th Five-Year Plan Overview*.

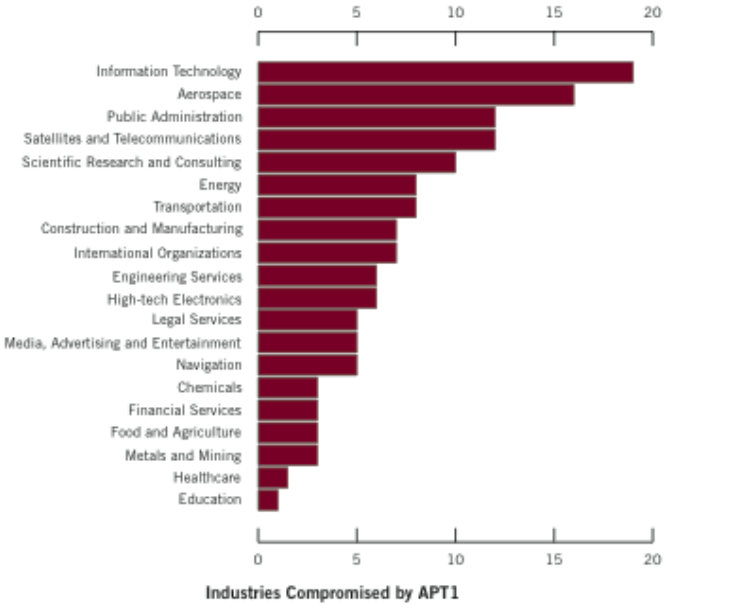

FIGURE 13: Number of APT1 victims by industry. We determined each organization's industry based on reviewing its industry classification in the Hoover's[29] system. We also considered the content of the data that APT1 stole in each case, to the extent that this information was available.

Figure 13. Mandiant's 2013 reporting of Chinese targeted cyber-espionage industrial areas [105]

China's strategic objectives as outlined in successive Five-Year Plans, 1986 through 2005, have targeted key U.S. research and development industrial areas, these industrial areas are also the same areas that have been targeted by China's cyber-espionage unit 61398.

Discussion & Implications

Photographs of the Chinese Shenyang Aircraft Corporation's (SAC) J-31 bare a striking similarity to the U.S.' F-35 Joint Strike Fighter. [106] If China has compromised the F-35 program via cyber-espionage, the United States has lost over $300 billion of

[105] Mandiant. *APT1: Exposing One of China's Cyber Espionage Units.*

[106] David Axe. "China's Newest Stealth Fighter Takes Flight," *Wired,* October 31, 2012, accessed June 21, 2014, http://www.wired.com/dangerroom/2012/10/china-stealth-first-flight/
.

research and development, not including losses in foreign sales, as well as considerable military advantage in the realm of stealth technology. [107]

Figure 14. China's J-31 Stealth Fighter [108]

[107] Defense Industry Daily. "The F-35's Air-to-Air Capability Controversy," October 12, 2008, accessed June 21, 2014, http://www.defenseindustrydaily.com/The-F-35s-Air-to-Air-Capability-Controversy-05089/.

[108] Axe. "China's Newest Stealth…"

Figure 15. The U.S. F-35 Stealth Fighter [109]

U.S. national leadership recognizes cyber security "as one of the most serious economic and national security challenges," while conceding further that the United States is not prepared to counter the current threat. [110] The U.S. military's "global communications backbone… consists of 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries." [111] This extensive information technology infrastructure, which does not include private industry that supports the military or broader government, facilitates U.S. military command and control but also logistical support, real-time provision of intelligence to forward forces in

[109] Defense Industry Daily. "The F-35's …"

[110] Executive Office of the President of the United States of America, "The Comprehensive National Cybersecurity Initiative," accessed August11, 2014, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[111] Lynn, "Defending a New Domain," 98.

austere environments, and general communications. [112] The U.S. military, government, and economy are reliant on cyberspace, the Internet, and related IT for a preponderance of day-to-day functions.

The PRC's focus on building high-tech industries and industrial manufacturing capacity, as outlined in successive Five-Year Plans as well as their National R&D Program (863), has led to a whole of government approach to technology acquisition in support of economic development. In answering the question - How can we prove that China's strategic Five-Year Plans drive the use of covert military assets (i.e. the People's Liberation Army) as tools to equip Chinese industry with economic advantage at the detriment of U.S. industry and interests? – one needs simply to compare what China's says its interests, goals, and objectives are with what the nation is investing in and pursuing.

China's strategic communication through their Five-Year Plan cycle goals coupled with proven espionage cases (indicted U.S. prosecutions), and attributed military supported cyber-espionage shows a powerful link between Chinese strategic doctrine and the leveraging of state tools and capabilities in order to meet national objectives. China's strategic aspiration is to increase its world economic standing and the standard of living for its people. China's high-technology output, a major factor in bolstering China's economic standing, has been steadily increasing for more than a decade (beyond that of peer competitors, see Figure 16). [113]

[112] Ibid., 98.

[113] David Wertime, "It's Official: China Is Becoming a New Innovation Powerhouse."

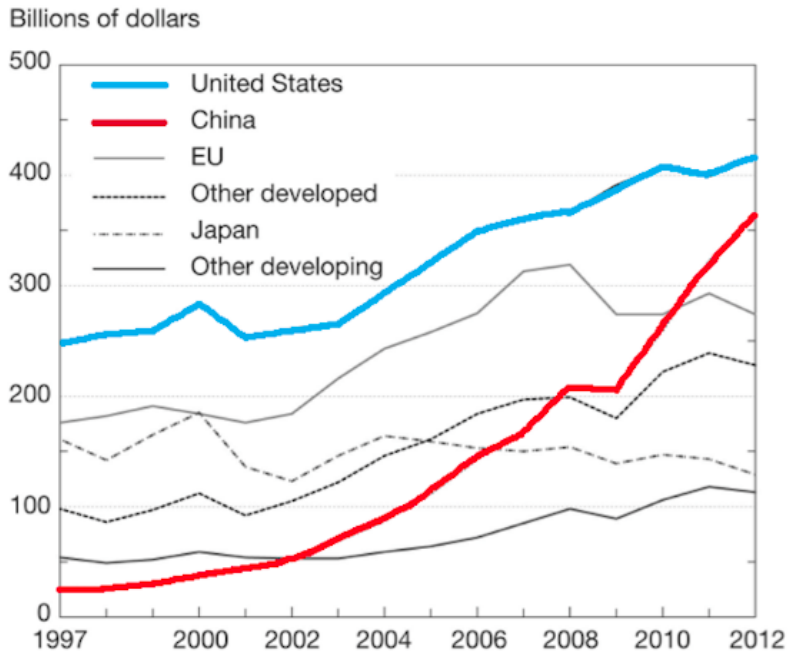

Figure 16. High-technology output since 1997 [114]

In spite of this, China remains a nation that relies on the acquisition of foreign technology and dual-use technology as a means to support and augment its lack of indigenous research and development. [115]

In order to meet ambitious goals set fourth in its strategic communication China must obtain development advantage by acquiring intellectual property relating to high-technology sectors through any means possible. China will continue to leverage a whole of government approach to acquire high-tech IP that will leverage the military and cyber-espionage as a means to obtain high volumes of data and IP quickly. Unlike the West, it makes sense for China to leverage the military in support of national economic interests.

[114] Ibid.

[115] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2014*.

Where the state owns the preponderance of the enterprise why would it not use all tools to ensure success?

China's communication of its strategic goals and objectives via its Five-Year Plans offers U.S. industry an opportunity to prepare and protect its critical industries and intellectual property against theft and exploitation via cyber-espionage. China has demonstrated that both its traditional as well as its cyber-espionage interests are aligned to meeting the high-tech industrial capabilities and goals communicated by their Five-Year Plans.

Summary Evaluation of Hypothesis Three

One could argue that the evidence is circumstantial; however, the People's Republic of China has demonstrated that in order to meet the goals and objectives set forward in their strategic Five-Year Plans, the PRC will leverage all aspects of their government in order to achieve success, including military supported cyber exploitation and intellectual property theft. U.S. industry can leverage the industrial development and concentration areas outlined in China's Five-Year Plans as focus areas China will be target for cyber exploitation and theft in order to close high-tech shortfalls and spur PRC information advantage.

This thesis has established a relationship between traditional Chinese espionage and attributed cyber exploitation and theft over time. This relationship was established by linking, mapping, and correlating U.S. indicted and tried Chinese espionage cases targeting high-technology information and industry areas identified in Chinese Five Year Plans with Chinese attributed cyber exploitation and theft against the same high-technology and industry areas. As U.S. indictments against Chinese nationals rose over

time so did Chinese attributed cyber exploitation. Chinese cyber exploitation and intellectual property theft began to replace traditional human enabled information gathering following peak Chinese indictments in 2008, with Chinese attributed cyber theft reaching its peak in 2013, a year that saw no indictments for Chinese espionage against key industrial areas. China's shift from traditional human-enabled espionage and information gathering to cyber-enabled virtual collection shows a logical movement towards gathering information that is difficult to indict, leveraging technology and resulting in collection of information that is low risk and high gain. There is opportunity for U.S. industry to protect itself from this cyber exploitation and intellectual property theft by hardening and protecting the key information and industrial growth areas China indentifies in its Five Year Plans.

Increasingly the use of China's military to conduct this intellectual property theft via cyberspace has muddied the waters. Although not covered in the examination and breadth of the work, I would argue that China's ultimate goal might not to be to target U.S. industry in order to obtain military defensive or offensive advantage, but to close technological gaps in order to obtain economic supremacy. China seems to be striving to evolve beyond being the world's factory to become the innovative, high technology, research and development market of the globe. This area could benefit from further analysis.

If China can achieve becoming the research and development hub of the world, it may be able to leverage high-technology manufacturing as a means to surpass the United States in intellectual capital creation, moving beyond the need for a military deterrent against U.S. intervention. If China can further secure its economic supremacy by

building alliances and dependencies based on defense export relationships, it will bolster its regional independence through market shares and trade. The PRC's targeting of U.S. high-technology areas is perhaps the beginning of efforts to undermine U.S. global exports and defense trade relations, as a means to obtain international favor within the globalized voting system of the current world order.

CHAPTER 5: CONCLUSION

How is cyberspace changing modern defense? Is cyberspace an operational domain of warfare or simple domain-like? This thesis explored these questions by deconstructing the major issues surrounding cyberspace into three focus areas.

The three topics explored, which corresponded to chapters two, three, and four of this work in order, were:

(4) How does the evolution of cyberspace compare with aerospace as it relates to U.S. military demonstrations of domain power (i.e. cyber power versus air power)?

(5) How does the U.S. Department of Defense compete with the private sector in the recruitment of the technical expertise needed to develop cyber warriors?

(6) How does the Peoples Republic of China's strategic Five-Year Plans drive their exploitation of cyberspace**?**

Firstly, this work examined cyberspace as a domain of warfare akin to land, sea, air, and space exploring whether it is or is not the latest addition. Exploring this concept proved exceptionally important to this study, as all current defense discourse asserts that cyberspace is in deed the fifth operational domain of warfare. However, contrary to this assertion this work concluded that cyberspace is not yet an operational domain of warfare in the traditional sense, but domain-like. The major implication of this finding is that the domain cyberspace and its associated cyber power is currently being leveraged as an enabler of warfare, and as a tool for the influence fight (i.e. mainly reconnaissance, information gathering, and preparation of the traditional battlefields of land, sea, air, and space).

Secondly, as a means to better understand cyberspace as a United States Department of Defense warfare domain, chapter three explored the recruitment of U.S.

cyber warriors. What better way to understand the defense aspects of cyberspace than to examine the expertise and background of those individuals being recruited to fight its wars? Although, there was not a lot of information readily available within this topic area, the research was able to identify key impediments that may restrict or hinder the diverse recruitment of future warriors including a potential shortage of technically qualified personnel for the DoD to leverage due to low graduation rates and anticipated 16 percent private sector growth rates through 2022 culminating in over a million private sector jobs, which are almost ensured to pay more than government or DoD service.

Thirdly, in the examination of a current example of how a nation state is leveraging cyberspace, and a potential future adversary for which warfare could be an option, chapter four of this work explored The People's Republic of China's (PRC) exploitation of cyberspace. The findings in this chapter indeed show that the PRC is exploiting cyberspace, but uncovered no direct linkages to or evidence of China's use of cyber weapons, but instead intellectual property theft in the guise of state sponsored corporate espionage.

In concert, the various finding of this study have helped to assert that within the discourse of national defense cyberspace is currently optimized for the influence fight and not traditional kinetic warfare as historically seen in the domains of land, sea, air, and space. Further research is needed to reexamine this assertion if cyberspace, through a myriad of non-kinetic exploits or capabilities, can be leveraged to create a defensive or offensive capability that is attributable, known and seen by the world, to a specific force (non-state actor) or nation state in the future.

Overall this thesis has argued that for cyberspace to be a true operational domain of warfare, akin to land, sea, air, or space, and not simply domain-like, that credible and attributed capability to an actor must be demonstrated in order for said capability to have a military coercive or deterrent effect that could be leveraged by policy makers. Further, as it relates to defense and deterrence, it is paramount for offensive or defensive military manipulation of cyberspace as a weapon of war to be surmised or known, and demonstrated or credible, in order for it to begin to earn a level understanding as a distinct military capability. As previously stated, simply leveraging cyberspace to obtain information or steal secrets, an evolution of espionage tradecraft and not warfare, does not constitute a new operational domain of warfare, as has been argued and stated in strategic global defense communication.

BIBLIOGRAPHY

Alperovitch, Dmitiri. *Revealed: Operation Shady RAT.* McAffee, n.d. Accessed October 11, 2013. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

APT1: Exposing One of China's Cyber Espionage Units. Mandiant, 2013. Accessed October 4, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy*, Vol 12, No. 2, Spring (1993): 141-165.

Axe, David. "China's Newest Stealth Fighter Takes Flight," *Wired,* October 31, 2012. Accessed June 21, 2014. http://www.wired.com/dangerroom/2012/10/china-stealth-first-flight/

Bloomberg Businessweek. "How a Spy Agency Recruits Future Cyber Warriors." *Bloomberg Businessweek Videos*, 2:00, March, 17, 2014, http://www.businessweek.com/videos/2014-03-17/how-a-spy-agency-recruits-future-cyber-warriors

Booth, William and Ruth Eglash. "Young Israeli cyberwarriors learn to duel in the dark." The Washington Post, October 8, 2014. Accessed October 12, 2014. http://www.washingtonpost.com/world/young-israeli-cyberwarriors-learn-to-duel-in-the-dark/2014/10/07/e07a9031-1e01-4815-8938-5fab87495e82_story.html

British Chamber of Commerce in China. "China's Twelfth Five Year Plan (2011-2015) – the Full English Version." British Chamber of Commerce in China. http://www.britishchamber.cn/content/chinas-twelfth-five-year-plan-2011-2015-full-english-version.

Cabinet Office, United Kingdom. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.* London: Cabinet Office, 2011.

Cain, Anthony Christopher. *The Forgotten Air Force: French Air Doctrine in the 1930s*. Washington, D.C.: Smithsonian Institution Press, 2002.

Cheung, Tai Ming, editor. *China's Emergence as a Defense Technological Power.* London and New York: Routledge, 2013.

Cheung, Tai Ming, editor. *Forging China's Military Might: A New Framework for Assessing Innovation.* Baltimore: Johns Hopkins University Press, 2014.

Cheung, Tai Ming. *Fortifying China: The Struggle to Build a Modern Defense Economy*. Ithaca and London: Cornell University Press, 2009.

China Briefing. "China Releases 12th Five-Year Plan for Trade in Electromechanical and High-Tech Products," June 7, 2012. Accessed June 21, 2014. http://www.china-briefing.com/news/2012/06/07/china-releases-12th-five-year-plan-for-trade-in-electromechanical-and-high-tech-products.html

China.org.cn. "The 7th Five Year Plan (1986-1990). Accessed June 21, 2014. http://www.china.org.cn/english/MATERIAL/157620.htm

Chun, Clayton K.S. *Aerospace Power in the Twenty-first Century: A Basic Primer*. Colorado Springs, CO: United States Air Force Academy, 2001.

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins Publishers, 2010.

Datoc, Christian. "The (Not So) Thin Red Line: Army Set To Change Phys. Requirements For 'Cyber Warriors'." *The Daily Caller*, October 28, 2014. Accessed November 4, 2014. http://dailycaller.com/2014/10/28/the-not-so-thin-red-line-army-set-to-change-phys-requirements-for-cyber-warriors/

Defense Industry Daily. "The F-35's Air-to-Air Capability Controversy." October 12, 2008. Accessed June 21, 2014, http://www.defenseindustrydaily.com/The-F-35s-Air-to-Air-Capability-Controversy-05089/.

Department of Defense, United States of America. *2012 Demographics Profile of the Military Community*. Department of Defense, 2012. Accessed November 4, 2014. http://www.militaryonesource.mil/12038/MOS/Reports/2012_Demographics_Report.pdf

Department of Defense, United States of America. *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to National Defense Authorization Act for Fiscal Year 2011, Section 934*. Washington, DC: U.S. Department of Defense, 2011.

Department of Defense, United States of America. *Department of Defense Diversity and Inclusion Strategic Plan 2012- 2017*. Department of Defense, 2012. Accessed October 10, 2014. http://diversity.defense.gov/Portals/51/Documents/DoD_Diversity_Strategic_Plan_%20final_as%20of%2019%20Apr%2012[1].pdf

Department of Defense, United States of America. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: U.S. Department of Defense, 2011.

Department of Defense, United States of America. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms.* Washington D.C.: U.S. Department of Defense, as amended through 15 October 2013.

Department of Justice, United States of America. "Press Releases 2006 to 2014." Accessed August 01, 2014. http://www.justice.gov/opa/pr/2014/August/.

Department of Labor, United State of America. "National Employment Matrix for Computer Programmers." *Bureau of Labor Statistics*. Accessed November 4, 2014. http://data.bls.gov/projections/nationalMatrix?queryParams=15-1131-143&ioType=o

Department of Labor, United State of America. "National Employment Matrix for Computer Systems Analysts." *Bureau of Labor Statistics*. Accessed November 4, 2014. http://data.bls.gov/projections/nationalMatrix?queryParams=15-1121-145&ioType=o

de Seversky, Alexander P. *Air Power: Key to Survival*. New York: Simon and Schuster, 1950.

Douhet, Giulio. *The Command of the Air*. Translated by Dino Ferrari. Washington, D.C.: Air Force History and Museums Program, 1998 (New York: Coward-McCann, 1942).

The Economist. "Cyberwar: War in the fifth domain." The Economist, July 1, 2010. Accessed October 20, 2013. http://www.economist.com/node/16478792.

Engebretson, Patrick. *The Basics of Hacking and Penetration Testing Second Edition: Ethical Hacking and Penetration Testing Made Easy*. Amsterdam: Elsevier, 2013.

Erickson, John. *Hacking: The Art of Exploitation 2nd Edition*. San Francisco: No Starch Press, 2008.

Espinel, Victoria A. *2013 Joint Strategic Plan on Intellectual Property Enforcement.* U.S. Intellectual Property Enforcement Coordinator, June 2013.

Executive Office of the President of the United States of America. "The Comprehensive National Cybersecurity Initiative." Accessed August 11, 2014, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Fairbank, John King. *The United States & China: Fourth Edition, Enlarged*. Cambridge, MA: Harvard University Press, 1983.

Fallows, James. "Cyber Warriors." The Atlantic, March 2010. Accessed October 12, 2014. http://www.theatlantic.com/magazine/archive/2010/03/cyber-warriors/307917/?single_page=true

Garamone, Jim. “Lynn: Cyberwarfare Extends Scope of Conflict.” Department of Defense. American Forces Press Service, October 1, 2010. Accessed November 7, 2013. http://www.defense.gov/news/newsarticle.aspx?id=61310.

Government Communications Headquarters, United Kingdom. *Executive Companion: 10 Steps to Cyber Security.* London: U.K. GCHQ, 2012.

Gu, Xiaolei. “China Releases Blueprint to Promote Seven Emerging Industries,” June 1, 2012. Accessed June 20, 2014. http://www.china-briefing.com/news/2012/06/01/china-releases-blueprint-to-promote-seven-emerging-industries.html

Hagel, Chuck. “Retirement Ceremony for General Keith Alexander.” Speech, Fort Meade, Md, March 28, 2014. Accessed October 8, 2014. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1837

Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology acquisition and military modernization*. London and New York: Routledge, 2013.

Harper, Allen, Jonathon Ness, Gideon Lenkey, Shon Harris, Chris Eagle, and Terron Williams. *Gray Hat Hacking: The Ethical Hacker’s Handbook Third Edition.* New York: McGraw Hill, 2011.

Hart, B. H. Liddell. *Strategy*. New York: Penguin Books, 1991 (London: Faber, 1967).

Healey, Jason, editor. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association, 2013.

Hilbert, Martin and Priscila López. "The World's Technological Capacity to Store, Communicate, and Compute Information.” Science, 2011, 332(6025), 60–65.

Hippler, Thomas. *Bombing the People: Giulio Douhet and the Foundations of Air-Power Strategy, 1884-1939*. Cambridge, UK: Cambridge University Press, 2013.

Huffington Post. “China Denies Hacking Operation.” Agence France Press, February 20, 2013. Accessed October 1, 2013. http://www.huffingtonpost.com/2013/02/20/china-denies-hacking_n_2722873.html.

Joint Chiefs of Staff, United States Department of Defense. “Joint Publication 3-12 (R) Cyberspace Operations.” Washington, D.C.: Joint Chiefs of Staff, February 2013.

KPMG. *China’s 12th Fiver-Year Plan Overview*. KPMG, March 2011. http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf

Kramer, Franklin D., Stuart H. Starr, and Larry K Wentz, editors. *Cyberpower and National Security.* Washington, D.C.: National Defense University Press and Potomac Books, Inc., 2009.

Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Northrop Grumman Corporation, March 7, 2012. http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf

Lawrence, Dune. "The U.S. Government Wants 6,000 New 'Cyber Warriors' by 2016." *Bloomberg Business Weekly*, April 15, 2014. Accessed October 12, 2014. http://www.businessweek.com/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare*. 1999. Reprint, Dehradun, India: Natrah Publishers, 2007.

Libbey, James K. *Alexander P. de Seversky and the Quest for Air Power.* Washington, D.C.: Potomac Books, 2013.

Libicki, Martin. "Cyberspace is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society*, v. 8, no. 2, Fall 2012: 325-340.

Lynn, III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, vol. 89, no. 5 (September/October 2010).

MacIsaac, David. "Voices from the Central Blue: The Air Power Theorists." In *Makers of Modern Strategy: From Machiavelli to the Nuclear Age,* edited by Peter Paret. Princeton, NJ: Princeton University Press, 1986.

Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. Mandiant, 2013. Accessed October 4, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Mann, James. *About Face: A History of America's Curious Relationship with China, from Nixon to Clinton*. New York: Vintage Books, 2000.

McCaney, Kevin. "Army proposes new classification for cyber warriors." *Defense Systems*, September 5, 2014. Accessed October 10, 2014. http://defensesystems.com/articles/2014/09/05/army-cyber-warrior-new-classification.aspx

McCaney, Kevin. "DOD budget reflects impact of cyber, unmanned systems, R&D." *Defense Systems*, March 4, 2014. Accessed October 10, 2014. http://defensesystems.com/articles/2014/03/04/dod-2015-budget-technology.aspx

McGarry, Brendan. "NSA Chief: What Cyberwarrior Shortage?" *Defenstech*, October 14, 2013. Accessed October 10, 2014. http://defensetech.org/2013/10/14/nsa-chief-what-cyberwarrior-shortage/

McNally, Kevin. "PMW 130 Overview for NDIA Briefing," May 11, 2011. Accessed May 5, 2014. http://www.slideserve.com/allie/pmw-130-overview-for-ndia

Military.com. "Are You Eligible to Join the Military?" *Military.com.* Accessed November 4, 2014. http://www.military.com/join-armed-forces/join-the-military-basic-eligibility.html

Ministry of Science and Technology of the People's Republic of China, "National High-tech (R&D) Program (863 Program)."Accessed July 7, 2014. http://www.most.gov.cn/eng/programmes1/200610/t20061009_36225.htm

Nakashima, Ellen. "Several nations trying to penetrate U.S. cyber-networks, says ex-FBI official." *The Washington Post*, April 18, 2012. Accessed October 2, 2013. http://www.washingtonpost.com/world/national-security/several-nations-trying-to-penetrate-us-cyber-networks-says-ex-fbi-official/2012/04/17/gIQAFAGUPT_story.html.

National Association of Manufacturers. "Facts About Manufacturing in the United States." Accessed July 10, 2014. http://www.nam.org/Statistics-And-Data/Facts-About-Manufacturing/Landing.aspx

National Center for Education Statistics. "Bachelor's degrees conferred by postsecondary institutions, by field of study: Selected years, 1970-71 through 2011-12." *Digest of Education Statistics*. Accessed October 12, 2014. http://nces.ed.gov/programs/digest/d13/tables/dt13_322.10.asp

National Center for Education Statistics. "Degrees in computer and information sciences conferred by degree-granting institutions, by level of degree and sex of student: 1970-71 through 2010-11." *Digest of Education Statistics*. Accessed October 12, 2014. http://nces.ed.gov/programs/digest/d12/tables/dt12_349.asp

Newman, Jonah. "Is There a Crisis in Computer-Science Education." *The Chronicle of Higher Education*, June 23, 2014. Accessed October 9, 2014. http://chronicle.com/blogs/data/2014/06/23/is-there-a-crisis-in-computer-science-education/

Nichols, Catherine. "Recruiting and developing the 21st century cyber warrior." *SC Magazine*, August 23, 2011. Accessed October 10, 2014. http://www.scmagazine.com/recruiting-and-developing-the-21st-century-cyber-warrior/article/210230/

Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011,* October 2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Office of the Press Secretary, The White House. "Executive Order 13583-- Establishing a Coordinated Government-wide Initiative to Promote Diversity and Inclusion in the Federal Workforce." The White House, August 18, 2011. Accessed October 10, 2014. http://www.whitehouse.gov/the-press-office/2011/08/18/executive-order-establishing-coordinated-government-wide-initiative-prom

Office of the Secretary of Defense, United States of America. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2014*. Office of the Secretary of Defense, 2014.

O'Hanlon, Michael. *The Wounded Giant: America's Armed Forces in an Age of Austerity*. New York: Penguin, 2011.

Pape, Robert A. *Bombing to Win: Air Power and Coercion in War*. Ithaca, N.Y.: Cornell University Press, 1996.

Patent and Trademark Office, United States of America. "Patent Counts by Origin and Type Calendar Year 2013." http://www.uspto.gov/web/offices/ac/ido/oeip/taf/st_co_13.htm

Pellerin, Cheryl. "Lynn: Cyberspace is the New Domain of Warfare." U.S. Department of Defense, October 18, 2010. Accessed October 20, 2013. http://www.defense.gov/news/newsarticle.aspx?id=61310.

People's Republic of China. "The 7th Five Year Plan (1986 – 1990)." China.org. http://www.china.org.cn/english/MATERIAL/157620.htm.

People's Republic of China. "The 8th Five-Year Plan (1991 – 1995)." China.org. http://www.china.org.cn/english/MATERIAL/157625.htm.

People's Republic of China. "The Ninth Five-Year Plan in Retrospect." China.org. http://www.china.org.cn/95e/index.html.

People's Republic of China. "The Tenth Five-Year Plan." China.org. http://www.china.org.cn/english/features/38198.htm.

People's Republic of China. "China Mapping out the 11th Five-Year Development Guidelines." China.org. http://www.china.org.cn/english/features/guideline/156529.htm.

Pillsbury, Michael. *China Debates the Future Security Environment*. Washington, D.C.: National Defense University Press, 2000.

Pillsbury, Michael editor. *Chinese Views of Future Warfare*. Honolulu, HI: university Press of the Pacific, 1977.

Rid, Thomas. *Cyber War Will Not Take Place.* New York: Oxford University Press, 2013.

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Random House, 2012.

Schreier, Fred. *On Cyberwarfare,* Geneva Center for the Democratic Control of Armed Forces Horizon 2015 Working Paper Series, no. 7 (2012).

Sherry, Michael S. *The Rise of American Air Power: The Creation of Armageddon*. New Haven, CT: Yale University Press, 1987.

Sternstin, Aliya. "Qualifying Cyber Command Staff is Harder Than You Think." *Nextgov*, April 14, 2014. Accessed October 10, 2014. http://www.nextgov.com/cybersecurity/2014/04/cyber-warrior-training-no-easy-task/82498/

Tate, Julie. "Report on 'Operation Shady RAT' identifies widespread cyber spying." Washington Post, July 29, 2011. Accessed July 9, 2014. http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html

Thomson, Iain. " US cyber-army's cyber-warriors cyber-humiliated by cyber-civvies in cyber-games." The Register, August 5, 2014. Accessed October 12, 2014. http://www.theregister.co.uk/2014/08/05/us_military_cyberwarriors_reservists_war_games/

Tyler, Patrick. *Six Presidents and China: A Great Wall; An Investigative History*. New York: Public Affairs, 2000.

Verizon. *2014 Data Breach Investigations Report*. Verizon, 2014. http://www.verizonenterprise.com/DBIR/2014/

Warner, Edward. "Douhet, Mitchell, Seversky: Theories of Air Warfare." In *Makers of Modern Strategy: Military Thought from Machiavelli to Hitler,* edited by Edward Earle. Princeton, NJ: Princeton University Press, 1948.

Weiwei, Xu. "China denies hacking claims." February 20, 2013. Accessed July 7, 2014. http://www.morningwhistle.com/html/2013/PoliticsSociety_0220/217214.html

Wertime, David. “It’s Official: China Is Becoming a New Innovation Powerhouse.” Foreign Policy, February 6, 2014. Accessed August 1, 2014. http://www.foreignpolicy.com/articles/2014/02/06/its_official_china_is_becoming_a_new_innovation_powerhouse.

CURRICULUM VITAE

Eric Allen Slate was born in Batavia, New York on May 30, 1981. He earned his Bachelors of Science degree in Aerospace Studies in 2011. At Johns Hopkins University, his academic studies focused on intelligence, security strategy, and cyber issues. A former United States Air Force intelligence specialist and a career civil servant, Mr. Slate is a noted government expert and speaker on maritime security, intelligence, and defense related topics, and has been the recipient of numerous awards and honors including two Department of Navy Meritorious Civilian Service Awards, the Department of Navy Award of Merit for Group Achievement, and the Office of the Director of National Intelligence Human Capital Outstanding Team Award.